

SIP

Mediant 1000

User's Manual Version 5.2



Table of Contents

| | | |
|----------|--|-----------|
| 1 | Overview | 19 |
| 1.1 | SIP Overview | 20 |
| 2 | Physical Description | 21 |
| 2.1 | Mediant 1000 Front Panel..... | 21 |
| 2.1.1 | I/O Modules | 23 |
| 2.1.2 | CPU Module | 24 |
| 2.1.2.1 | Dry Contact Connector (Labeled I and II) | 24 |
| 2.1.2.2 | Audio IN/OUT1 | 24 |
| 2.1.2.3 | 10/100 Base-TX Ethernet Ports (Labeled I and II)..... | 24 |
| 2.1.2.4 | RS-232 Port (Labeled IOIO) | 25 |
| 2.1.2.5 | Reset Button (Labeled //) | 25 |
| 2.1.3 | Media Process Module (MPM) | 25 |
| 2.1.4 | Power Supply Module (Labeled 1 and 2) | 25 |
| 2.1.5 | Fan Tray Module..... | 26 |
| 2.1.6 | Front Panel LEDs | 27 |
| 2.2 | Mediant 1000 Rear Panel | 29 |
| 3 | Installing the Mediant 1000..... | 31 |
| 3.1 | Unpacking | 31 |
| 3.2 | Package Contents..... | 31 |
| 3.3 | Mounting the Mediant 1000..... | 32 |
| 3.3.1 | Mounting Mediant 1000 on a Desktop..... | 32 |
| 3.3.2 | Installing Mediant 1000 in a 19-inch Rack..... | 34 |
| 3.4 | Cabling the Mediant 1000 | 35 |
| 3.4.1 | Grounding Mediant 1000 | 35 |
| 3.4.2 | Connecting to the Ethernet Network..... | 36 |
| 3.4.3 | Connecting to FXS / FXO Interfaces | 36 |
| 3.4.4 | Cabling the Analog Lifeline Phone | 37 |
| 3.4.5 | Connecting to Digital Trunks | 39 |
| 3.4.6 | Cabling the Digital Lifeline | 40 |
| 3.4.7 | Cabling the Dry Contact Relay Alarm System..... | 40 |
| 3.4.8 | Connecting the Mediant 1000 RS-232 Port to a PC..... | 42 |
| 3.4.9 | Connecting Mediant 1000 to Power | 42 |
| 3.5 | Maintenance..... | 42 |
| 3.5.1 | Replacing Modules | 43 |
| 3.5.2 | Inserting Modules into Previously Empty Slots | 44 |
| 3.5.3 | Replacing the Air Filter | 45 |
| 4 | Getting Started | 47 |
| 4.1 | Configuration Concepts..... | 47 |
| 4.2 | Startup Process..... | 48 |
| 4.3 | Assigning an IP Address..... | 50 |
| 4.3.1 | Assigning an IP Address Using HTTP..... | 50 |
| 4.3.2 | Assigning an IP Address Using BootP | 51 |
| 4.3.3 | Assigning an IP Address Using the Voice Menu Guidance..... | 52 |

| | | |
|----------|--|-----------|
| 4.3.4 | Assigning an IP Address Using the CLI..... | 53 |
| 4.3.4.1 | Accessing the CLI | 53 |
| 4.3.4.2 | Assigning an IP Address | 54 |
| 4.4 | Configuring Basic Parameters | 55 |
| 5 | Web-based Management | 57 |
| 5.1 | Computer Requirements | 57 |
| 5.2 | Protection and Security Mechanisms | 57 |
| 5.2.1 | User Accounts | 58 |
| 5.2.2 | Limiting the Embedded Web Server to Read-Only Mode | 59 |
| 5.2.3 | Disabling the Embedded Web Server | 59 |
| 5.3 | Accessing the Embedded Web Server | 60 |
| 5.4 | Getting Acquainted with the Web Interface | 61 |
| 5.4.1 | Main Menu Bar | 62 |
| 5.4.2 | Saving Changes | 62 |
| 5.4.3 | Entering Phone Numbers in Various Tables | 62 |
| 5.4.4 | Searching for Configuration Parameters | 63 |
| 5.4.5 | Customizing the Web Interface | 65 |
| 5.4.5.1 | Replacing the Main Corporate Logo | 65 |
| 5.4.5.2 | Replacing the Background Image File | 68 |
| 5.4.5.3 | Customizing the Product Name | 69 |
| 5.4.5.4 | Creating a Login Welcome Message | 70 |
| 5.5 | Protocol Management | 71 |
| 5.5.1 | Protocol Definition Parameters | 71 |
| 5.5.1.1 | General Parameters | 72 |
| 5.5.1.2 | Proxy & Registration Parameters | 84 |
| 5.5.1.3 | Coders | 94 |
| 5.5.1.4 | DTMF & Dialing Parameters | 98 |
| 5.5.2 | Configuring the Advanced Parameters | 102 |
| 5.5.2.1 | General Parameters | 103 |
| 5.5.2.2 | Supplementary Services | 113 |
| 5.5.2.3 | Metering Tones | 118 |
| 5.5.2.4 | Keypad Features | 120 |
| 5.5.2.5 | Stand-Alone Survivability | 123 |
| 5.5.3 | Configuring the Number Manipulation Tables | 125 |
| 5.5.3.1 | Dialing Plan Notation | 128 |
| 5.5.3.2 | Numbering Plans and Type of Number | 129 |
| 5.5.3.3 | Mapping NPI/TON to Phone-Context | 130 |
| 5.5.4 | Configuring the Routing Tables | 132 |
| 5.5.4.1 | General Parameters | 132 |
| 5.5.4.2 | Tel to IP Routing Table | 134 |
| 5.5.4.3 | IP to Trunk Group Routing | 138 |
| 5.5.4.4 | Internal DNS Table | 140 |
| 5.5.4.5 | Internal SRV Table | 141 |
| 5.5.4.6 | Reasons for Alternative Routing | 142 |
| 5.5.4.7 | Release Cause Mapping | 144 |
| 5.5.5 | Configuring the Profile Definitions | 144 |
| 5.5.5.1 | Coder Group Settings | 145 |
| 5.5.5.2 | Tel Profile Settings | 146 |
| 5.5.5.3 | IP Profile Settings | 148 |
| 5.5.6 | Configuring the Trunk Group Table | 150 |
| 5.5.7 | Configuring the Trunk Group Settings | 152 |
| 5.5.8 | Configuring the Endpoint Settings | 154 |
| 5.5.8.1 | Authentication | 154 |
| 5.5.8.2 | Automatic Dialing | 155 |
| 5.5.8.3 | Caller ID | 156 |

| | | |
|----------|--|-----|
| 5.5.8.4 | Call Forward | 157 |
| 5.5.8.5 | Caller ID Permissions | 159 |
| 5.5.8.6 | Call Waiting | 160 |
| 5.5.9 | Configuring the Digital Gateway Parameters | 161 |
| 5.5.10 | Configuring the Advanced Applications | 166 |
| 5.5.10.1 | Configuring RADIUS Accounting Parameters | 166 |
| 5.5.10.2 | Configuring the FXO Parameters | 168 |
| 5.5.10.3 | Configuring the Voice Mail (VM) Parameters | 172 |
| 5.5.11 | Configuring the IPmedia Parameters | 175 |
| 5.6 | Network Settings | 178 |
| 5.6.1 | Configuring the IP Settings | 178 |
| 5.6.2 | Configuring the Application Settings | 182 |
| 5.6.3 | Configuring the NFS Settings | 184 |
| 5.6.4 | Configuring the IP Routing Table | 186 |
| 5.6.5 | Configuring the VLAN Settings | 188 |
| 5.7 | Media Settings | 190 |
| 5.7.1 | Configuring the Voice Settings | 191 |
| 5.7.2 | Configuring the Fax / Modem / CID Settings | 194 |
| 5.7.3 | Configuring the RTP / RTCP Settings | 198 |
| 5.7.4 | Configuring the IPmedia Settings | 202 |
| 5.7.5 | Configuring the Hook-Flash Settings | 204 |
| 5.7.6 | Configuring the General Media Settings | 205 |
| 5.8 | PSTN Settings | 206 |
| 5.8.1 | Configuring the PSTN Settings | 206 |
| 5.8.1.1 | Trunk Settings | 206 |
| 5.8.1.2 | CAS State Machines | 219 |
| 5.8.2 | Configuring the TDM Bus Settings | 221 |
| 5.9 | Security Settings | 223 |
| 5.9.1 | Configuring the Web User Accounts | 223 |
| 5.9.2 | Configuring the Web and Telnet Access List | 225 |
| 5.9.3 | Configuring the Firewall Settings | 226 |
| 5.9.4 | Configuring the Certificates | 228 |
| 5.9.4.1 | Server Certificate Replacement | 228 |
| 5.9.4.2 | Client Certificates | 229 |
| 5.9.4.3 | Self-Signed Certificates | 231 |
| 5.9.5 | Configuring the General Security Settings | 232 |
| 5.9.6 | Configuring the IPSec Table | 236 |
| 5.9.7 | Configuring the IKE Table | 240 |
| 5.10 | Configuring the Management Settings | 243 |
| 5.10.1 | Configuring the SNMP Trap Destinations Table | 246 |
| 5.10.2 | Configuring the SNMP Community Strings | 248 |
| 5.10.3 | Configuring SNMP V3 Users | 249 |
| 5.11 | Status & Diagnostics | 251 |
| 5.11.1 | Gateway Statistics | 251 |
| 5.11.1.1 | IP Connectivity | 251 |
| 5.11.1.2 | Call Counters | 254 |
| 5.11.1.3 | Call Routing Status | 256 |
| 5.11.1.4 | SAS Registered Users | 257 |
| 5.11.2 | Activating the Internal Syslog Viewer | 258 |
| 5.11.3 | Device Information | 259 |
| 5.11.4 | Viewing the Ethernet Port Information | 260 |
| 5.11.5 | Viewing Performance Statistics | 261 |

| | | |
|----------|---|------------|
| 5.12 | Software Update | 262 |
| 5.12.1 | Software Upgrade Wizard..... | 262 |
| 5.12.2 | Automatic Update Mechanism..... | 266 |
| 5.12.3 | Auxiliary Files..... | 269 |
| 5.12.3.1 | Loading the Auxiliary Files via the Embedded Web Server | 270 |
| 5.12.3.2 | Loading the Auxiliary Files via the ini File | 271 |
| 5.12.4 | Updating the Software Upgrade Key | 271 |
| 5.12.4.1 | Backing up the Current Software Upgrade Key | 272 |
| 5.12.4.2 | Loading the Software Upgrade Key | 272 |
| 5.12.4.3 | Verifying that the Key was Successfully Loaded | 275 |
| 5.12.4.4 | Troubleshooting an Unsuccessful Loading of a Key | 275 |
| 5.13 | Maintenance..... | 276 |
| 5.13.1 | Regional Settings..... | 276 |
| 5.13.2 | Locking and Unlocking the Gateway | 276 |
| 5.13.3 | Saving Configuration | 278 |
| 5.13.4 | Resetting the Gateway | 279 |
| 5.13.5 | Restoring and Backing up Configuration | 280 |
| 5.13.6 | Factory Default Settings | 281 |
| 5.13.6.1 | Defining Default Values..... | 281 |
| 5.13.6.2 | Restoring Default Settings | 282 |
| 5.14 | Using the Home Page | 282 |
| 5.14.1 | Accessing the Home Page | 282 |
| 5.14.2 | Monitoring the Mediant 1000 Trunks and Channels..... | 284 |
| 5.14.3 | Monitoring the Modules | 287 |
| 5.14.4 | Monitoring Ethernet Ports, Dry Contacts, Power Supply Units, and Fan Tray Unit..... | 288 |
| 5.14.5 | Viewing the Active Alarms Table | 288 |
| 5.14.6 | Viewing Ethernet Port Information..... | 289 |
| 5.14.7 | Assigning a Name or Brief Description to a Port..... | 290 |
| 5.14.8 | Releasing an Analog Channel..... | 290 |
| 5.14.9 | Replacing Modules | 290 |
| 5.15 | Logging Off the Embedded Web Server | 292 |
| 6 | ini File Configuration | 293 |
| 6.1 | Secured ini File | 293 |
| 6.2 | Modifying an ini File | 293 |
| 6.3 | The ini File Content..... | 294 |
| 6.4 | The ini File Structure | 294 |
| 6.4.1 | The ini File Structure Rules | 295 |
| 6.4.2 | Structure of Individual ini File Parameters..... | 295 |
| 6.4.3 | Structure of ini File Parameter Tables | 295 |
| 6.4.4 | The ini File Example | 298 |
| 6.5 | The ini File Parameter Reference | 298 |
| 6.5.1 | Networking Parameters | 299 |
| 6.5.2 | System Parameters | 308 |
| 6.5.3 | Web and Telnet Parameters..... | 315 |
| 6.5.4 | Security Parameters | 318 |
| 6.5.5 | RADIUS Parameters..... | 320 |
| 6.5.6 | SNMP Parameters..... | 321 |
| 6.5.7 | SIP Configuration Parameters..... | 323 |
| 6.5.8 | Media Server Parameters..... | 337 |
| 6.5.9 | Voice Mail Parameters..... | 338 |
| 6.5.10 | PSTN Parameters..... | 340 |
| 6.5.11 | ISDN and CAS Interworking-Related Parameters..... | 343 |
| 6.5.12 | Analog Telephony Parameters | 350 |

| | | |
|----------|---|------------|
| 6.5.13 | Number Manipulation and Routing Parameters | 359 |
| 6.5.14 | Channel Parameters..... | 372 |
| 6.5.15 | Configuration Files Parameters | 378 |
| 7 | Telephony Capabilities | 379 |
| 7.1 | Configuring the DTMF Transport Types..... | 379 |
| 7.2 | Fax and Modem Capabilities..... | 380 |
| 7.2.1 | Fax/Modem Operating Modes | 380 |
| 7.2.2 | Fax/Modem Transport Modes | 381 |
| 7.2.2.1 | T.38 Fax Relay Mode | 381 |
| 7.2.2.2 | Fax/Modem Bypass Mode | 382 |
| 7.2.2.3 | Fax / Modem NSE Mode | 383 |
| 7.2.2.4 | G.711 Fax / Modem Transport Mode | 384 |
| 7.2.2.5 | Fax Fallback | 384 |
| 7.2.2.6 | Fax / Modem Transparent Mode | 385 |
| 7.2.2.7 | Fax / Modem Transparent with Events Mode | 385 |
| 7.2.3 | Supporting V.34 Faxes | 386 |
| 7.2.3.1 | Using Bypass Mechanism for V.34 Fax Transmission..... | 386 |
| 7.2.3.2 | Using Relay mode for both T.30 and V.34 faxes | 386 |
| 7.2.4 | Supporting V.152 Implementation | 387 |
| 7.3 | FXO Operating Modes | 388 |
| 7.3.1 | IP-to-Telephone Calls | 388 |
| 7.3.1.1 | One-Stage Dialing | 388 |
| 7.3.1.2 | Two-Stage Dialing | 390 |
| 7.3.1.3 | Call Termination (Disconnect Supervision) on Mediant 1000/FXO | 390 |
| 7.3.1.4 | DID Wink | 392 |
| 7.3.2 | Telephone-to-IP Calls | 392 |
| 7.3.2.1 | Automatic Dialing | 392 |
| 7.3.2.2 | Collecting Digits Mode..... | 393 |
| 7.3.2.3 | Ring Detection Timeout..... | 394 |
| 7.3.2.4 | FXO Supplementary Services | 394 |
| 7.4 | Event Notification using X-Detect Header | 394 |
| 7.5 | RTP Multiplexing (ThroughPacket) | 396 |
| 7.6 | Dynamic Jitter Buffer Operation | 397 |
| 7.7 | Configuring Alternative Routing (Based on Connectivity and QoS) | 398 |
| 7.7.1 | Alternative Routing Mechanism..... | 398 |
| 7.7.2 | Determining the Availability of Destination IP Addresses..... | 398 |
| 7.7.3 | PSTN Fallback as a Special Case of Alternative Routing | 399 |
| 7.7.4 | Relevant Parameters | 399 |
| 7.8 | Mapping PSTN Release Cause to SIP Response | 399 |
| 7.9 | Call Detail Record | 400 |
| 7.10 | Supported RADIUS Attributes..... | 402 |
| 7.10.1 | RADIUS Server Messages | 404 |
| 7.11 | Trunk-to-Trunk Routing Example | 404 |
| 7.12 | Proxy or Registrar Registration Example | 405 |
| 7.13 | Configuration Examples | 406 |
| 7.13.1 | SIP Call Flow | 406 |
| 7.13.2 | SIP Authentication Example | 409 |
| 7.13.3 | Establishing a Call between Two gateways | 411 |
| 7.13.4 | Remote IP Extension between FXO and FXS | 412 |
| 7.13.4.1 | Dialing from Remote Extension (Phone Connected to FXS) | 412 |
| 7.13.4.2 | Dialing from other PBX line, or from PSTN | 413 |

| | | |
|----------|---|------------|
| 7.13.4.3 | FXS Gateway Configuration (using the Embedded Web Server) | 413 |
| 7.13.4.4 | FXO Gateway Configuration (using the Embedded Web Server) | 414 |
| 7.14 | Working with Supplementary Services | 415 |
| 7.14.1 | Call Hold and Retrieve | 415 |
| 7.14.2 | Consultation / Alternate | 416 |
| 7.14.3 | Call Transfer | 416 |
| 7.14.4 | Call Forward | 417 |
| 7.14.5 | Call Waiting | 418 |
| 7.14.6 | Message Waiting Indication | 418 |
| 7.14.7 | Caller ID | 419 |
| 7.14.7.1 | Caller ID Detection / Generation on the Tel Side | 419 |
| 7.14.7.2 | Debugging a Caller ID Detection on FXO | 420 |
| 7.14.7.3 | Caller ID on the IP Side | 421 |
| 8 | Networking Capabilities | 423 |
| 8.1 | Ethernet Interface Configuration | 423 |
| 8.2 | Ethernet Interface Redundancy | 423 |
| 8.3 | NAT (Network Address Translation) Support | 424 |
| 8.3.1 | STUN | 425 |
| 8.3.2 | First Incoming Packet Mechanism | 426 |
| 8.3.3 | No-Op Packets | 426 |
| 8.4 | Point-to-Point Protocol over Ethernet (PPPoE) | 427 |
| 8.4.1 | Point-to-Point Protocol (PPP) Overview | 427 |
| 8.4.2 | PPPoE Overview | 428 |
| 8.4.3 | PPPoE in AudioCodes Gateway | 428 |
| 8.5 | IP Multicasting | 429 |
| 8.6 | Robust Reception of RTP Streams | 429 |
| 8.7 | Multiple Routers Support | 429 |
| 8.8 | Simple Network Time Protocol Support | 430 |
| 8.9 | IP QoS via Differentiated Services (DiffServ) | 430 |
| 8.10 | VLANs and Multiple IPs | 431 |
| 8.10.1 | Multiple IPs | 431 |
| 8.10.2 | IEEE 802.1p/Q (VLANs and Priority) | 431 |
| 8.10.3 | Getting Started with VLANs and Multiple IPs | 434 |
| 8.10.3.1 | Integrating Using the Embedded Web Server | 434 |
| 8.10.3.2 | Integrating Using the ini File | 437 |
| 9 | Advanced PSTN Configuration | 439 |
| 9.1 | Clock Settings | 439 |
| 9.2 | Release Reason Mapping | 440 |
| 9.2.1 | Reason Header | 440 |
| 9.2.2 | Fixed Mapping of ISDN Release Reason to SIP Response | 441 |
| 9.2.3 | Fixed Mapping of SIP Response to ISDN Release Reason | 443 |
| 9.3 | ISDN Overlap Dialing | 444 |
| 9.4 | Using ISDN NFAS | 445 |
| 9.4.1 | NFAS Interface ID | 445 |
| 9.4.2 | Working with DMS-100 Switches | 446 |
| 9.4.3 | Creating an NFAS-Related Trunk Configuration On-The-Fly | 447 |
| 9.5 | Redirect Number and Calling Name (Display) | 448 |

| | |
|--|------------|
| 10 Media Server Capabilities | 449 |
| 10.1 Conference Server | 449 |
| 10.1.1 Simple Conferencing (NetAnn) | 450 |
| 10.1.1.1 SIP Call Flow | 450 |
| 10.1.1.2 Creating a Conference | 451 |
| 10.1.1.3 Joining a Conference | 451 |
| 10.1.1.4 Terminating a Conference | 451 |
| 10.1.1.5 PSTN Participants | 452 |
| 10.1.2 Advanced Conferencing (MSCML) | 452 |
| 10.1.2.1 Creating a Conference | 452 |
| 10.1.2.2 Joining a Conference | 453 |
| 10.1.2.3 Modifying a Conference | 454 |
| 10.1.2.4 Applying Media Services on a Conference | 454 |
| 10.1.2.5 Active Speaker Notification | 455 |
| 10.1.2.6 Terminating a Conference | 456 |
| 10.1.3 Conference Call Flow Example | 456 |
| 10.2 Announcement Server | 463 |
| 10.2.1 NetAnn Interface | 463 |
| 10.2.1.1 Playing a Local Voice Prompt | 463 |
| 10.2.1.2 Playing using HTTP/NFS Streaming | 463 |
| 10.2.1.3 Supported Attributes | 464 |
| 10.2.2 MSCML Interface | 464 |
| 10.2.2.1 Operation | 466 |
| 10.2.2.2 Playing Announcements | 467 |
| 10.2.2.3 Playing Announcements and Collecting Digits | 468 |
| 10.2.2.4 Playing Announcements and Recording Voice | 470 |
| 10.2.2.5 Stopping the Playing of an Announcement | 471 |
| 10.2.2.6 Relevant Parameters | 471 |
| 10.2.3 Announcement Call Flow Example | 472 |
| 10.3 IP-to-IP Transcoding | 474 |
| 11 Tunneling Applications | 477 |
| 11.1 TDM Tunneling | 477 |
| 11.1.1 Implementation | 477 |
| 11.2 QSIG Tunneling | 480 |
| 11.2.1 Implementation | 480 |
| 12 Selected Technical Specifications | 481 |
| 13 Supplied SIP Software Package | 485 |
| 14 OSN Server Hardware Installation | 487 |
| 14.1 Required Working Tools | 487 |
| 14.2 OSN Server Installation on the Mediant 1000 | 487 |
| 14.2.1 Installing the CM Module | 489 |
| 14.2.2 Installing the iPMX Module | 490 |
| 14.2.3 Installing the HDMX Module | 492 |
| 14.3 Replacing the iPMX Module's Lithium Battery | 492 |

| | | |
|-----------|---|------------|
| 15 | Installing Linux™ Operating System on the OSN Server | 495 |
| 15.1 | Requirements..... | 495 |
| 15.1.1 | Hardware | 495 |
| 15.1.2 | Software..... | 496 |
| 15.2 | Cabling | 496 |
| 15.3 | Installing Linux™ RedHat (and Fedora)..... | 497 |
| 15.3.1 | Stage 1: Obtaining the Linux Redhat ISO Image | 497 |
| 15.3.1.1 | Downloading an Updated ISO Image..... | 497 |
| 15.3.1.2 | Creating an Updated ISO Image..... | 497 |
| 15.3.2 | Stage 2: Editing the isolinux.cfg File..... | 500 |
| 15.3.3 | Stage 3: Burning ISO Image File to CD-ROM..... | 504 |
| 15.3.4 | Stage 4: Installing the Boot Media..... | 504 |
| 15.3.5 | Additional RedHat™ and Fedora™ Installation Notes | 506 |
| 15.3.6 | Post-installation Notes for Kernels 2.6+ (Fedora™ Core 4+ and RedHat™ EL 4+)..... | 506 |
| 15.4 | Installing Linux™ Debian | 507 |
| 15.4.1 | Stage 1: Obtaining the ISO Image..... | 507 |
| 15.4.2 | Stage 2: Preparing the Boot Media | 508 |
| 15.4.3 | Stage 3: Editing the isolinux.cfg File..... | 510 |
| 15.4.3.1 | Downloading an Updated Debian isolinux.cfg File..... | 510 |
| 15.4.3.2 | Editing the isolinux.cfg File..... | 510 |
| 15.4.4 | Stage 4: Burning ISO Image to CD | 513 |
| 15.4.5 | Stage 5: Installing the Boot Media..... | 513 |
| 15.4.6 | Additional Linux™ Debian Installation Notes | 514 |
| 15.5 | Installing Linux™ SUSE | 516 |
| 15.5.1 | Additional Requirement for Linux™ SUSE Installation..... | 516 |
| 15.5.2 | Stage 1: Obtaining the ISO Image..... | 516 |
| 15.5.3 | Stage 2: Preparing the Boot Media | 517 |
| 15.5.4 | Stage 3: Editing the isolinux.cfg File..... | 519 |
| 15.5.4.1 | Downloading an Updated SUSE isolinux.cfg File | 519 |
| 15.5.4.2 | Editing the isolinux.cfg File..... | 520 |
| 15.5.5 | Stage 4: Burning the CD..... | 523 |
| 15.5.6 | Stage 5: Installing the Boot Media..... | 524 |

List of Figures

| | |
|---|-----|
| Figure 2-1: Mediant 1000 Front View and CPU Enlargement..... | 21 |
| Figure 2-2: Mediant 1000 Front Layout..... | 22 |
| Figure 2-3: 4-Port FXS Analog Module..... | 23 |
| Figure 2-4: 4-Port FXO G (Ground Start) Analog Module..... | 23 |
| Figure 2-5: 4-Port FXO G (Ground Start) Analog Module..... | 23 |
| Figure 2-6: Digital Module (e.g., 2 Spans)..... | 23 |
| Figure 2-7: CPU Module..... | 24 |
| Figure 2-8: Media Process Module (MPM)..... | 25 |
| Figure 2-9: Power Supply Module..... | 26 |
| Figure 2-10: Fan Tray Module with Six Fans and an Air Filter..... | 26 |
| Figure 2-11: Location of Front Panel LEDs..... | 27 |
| Figure 2-12: Mediant 1000 Rear Connectors..... | 29 |
| Figure 3-1: Attached Rubber Foot on Underside of Chassis..... | 32 |
| Figure 3-2: Location of Grooves for Rubber Feet..... | 33 |
| Figure 3-3: Peeled-off Rubber Foot..... | 33 |
| Figure 3-4: RJ-45 Connector Pinouts..... | 36 |
| Figure 3-5: RJ-11 Connector Pinouts..... | 37 |
| Figure 3-6: RJ-11 Connector Pinouts for FXS Lifeline..... | 37 |
| Figure 3-7: Mediant 1000 Lifeline Setup..... | 38 |
| Figure 3-8: RJ-48c Connector Pinouts..... | 39 |
| Figure 3-9: Mediant 1000 Digital Lifeline Cabling (e.g., Trunks 1 and 2)..... | 40 |
| Figure 3-10: Dry Contact Wires' Mate..... | 41 |
| Figure 3-11: RS-232 Cable Adaptor..... | 42 |
| Figure 3-12: Slightly Extracted Fan Try Unit..... | 45 |
| Figure 3-13: Fan Tray with Filter Removed..... | 46 |
| Figure 4-1: Startup Process..... | 49 |
| Figure 4-2: Quick Setup Screen..... | 55 |
| Figure 5-1: Enter Network Password Screen..... | 60 |
| Figure 5-2: Areas of the Web-based User Interface..... | 61 |
| Figure 5-3: Searched Result Screen..... | 63 |
| Figure 5-4: Searched Parameter Highlighted in Screen..... | 64 |
| Figure 5-5: Customized Web Interface Title Bar..... | 65 |
| Figure 5-6: Customized Web Interface Title Bar..... | 65 |
| Figure 5-7: Image Download Screen..... | 66 |
| Figure 5-8: User-Defined Web Welcome Message after Login..... | 70 |
| Figure 5-9: General Parameters Screen (Protocol Definition Submenu)..... | 72 |
| Figure 5-10: Proxy & Registration Screen..... | 84 |
| Figure 5-11: Coders Screen..... | 95 |
| Figure 5-12: DTMF & Dialing Screen..... | 98 |
| Figure 5-13: General Parameters (Advanced Submenu)..... | 103 |
| Figure 5-14: Supplementary Services Screen..... | 113 |
| Figure 5-15: Metering Tones Parameters Screen..... | 119 |
| Figure 5-16: Charge Codes Table Screen..... | 120 |
| Figure 5-17: Keypad Features Screen..... | 121 |
| Figure 5-18: Stand-Alone Survivability Screen..... | 124 |
| Figure 5-19: Source Phone Number Manipulation Table for Tel-to-IP Calls..... | 126 |
| Figure 5-20: Phone Context Table Screen..... | 130 |
| Figure 5-21: Routing Tables - General Parameters Screen..... | 132 |
| Figure 5-21: Tel to IP Routing Screen..... | 136 |
| Figure 5-22: IP to Trunk Group Routing Table Screen..... | 139 |
| Figure 5-23: Internal DNS Table Screen..... | 141 |
| Figure 5-24: Internal SRV Table Screen..... | 142 |
| Figure 5-25: Reasons for Alternative Routing Screen..... | 143 |
| Figure 5-26: Release Cause Mapping Screen (e.g., ISDN to SIP)..... | 144 |
| Figure 5-27: Coder Group Settings Screen..... | 145 |

| | |
|--|-----|
| Figure 5-28: IP Profile Settings Screen | 149 |
| Figure 5-29: Trunk Group Settings Screen | 152 |
| Figure 5-30: Authentication Screen | 154 |
| Figure 5-31: Digital Gateway Parameters Screen | 161 |
| Figure 5-32: RADIUS Parameters Screen | 167 |
| Figure 5-33: FXO Settings Screen | 168 |
| Figure 5-34: Voice Mail Screen | 172 |
| Figure 5-35: IPmedia Parameters Screen | 175 |
| Figure 5-36: IP Settings Screen | 178 |
| Figure 5-37: Application Settings Screen | 182 |
| Figure 5-38: NFS Settings Screen | 185 |
| Figure 5-39: IP Routing Table Screen | 187 |
| Figure 5-40: VLAN Settings Screen | 188 |
| Figure 5-41: Fax / Modem / CID Settings Screen | 194 |
| Figure 5-42: IPmedia Settings Screen | 202 |
| Figure 5-43: Hook-Flash Settings Screen | 204 |
| Figure 5-44: General Media Settings Screen | 205 |
| Figure 5-45: Trunk Settings Screen | 206 |
| Figure 5-46: CAS State Machine Table Screen | 219 |
| Figure 5-47: TDM Bus Settings Screen | 221 |
| Figure 5-48: Web User Accounts Screen (for Users with 'Security Administrator' Privileges) | 224 |
| Figure 5-49: Web & Telnet Access List Screen | 225 |
| Figure 5-50: Firewall Settings Screen | 226 |
| Figure 5-51: Certificates Signing Request Screen | 228 |
| Figure 5-52: General Security Settings Screen | 232 |
| Figure 5-53: IPSec Table Screen | 236 |
| Figure 5-54: IKE Table Screen | 240 |
| Figure 5-55: Management Settings Screen | 243 |
| Figure 5-56: SNMP Trap Destinations Screen | 246 |
| Figure 5-57: SNMP Community Strings Screen | 248 |
| Figure 5-58: SNMP V3 Setting Screen | 249 |
| Figure 5-59: IP Connectivity Screen | 252 |
| Figure 5-60: Calls Count Screen (e.g., Tel to IP) | 254 |
| Figure 5-61: Call Routing Status Screen | 256 |
| Figure 5-62: SAS Registered Users Screen | 257 |
| Figure 5-63: Message Log Screen | 258 |
| Figure 5-64: Basic Statistics Screen | 261 |
| Figure 5-65: Start Software Upgrade Wizard Screen | 263 |
| Figure 5-66: End Process Wizard Screen | 266 |
| Figure 5-67: Auxiliary Files Screen | 270 |
| Figure 5-68: Software Upgrade Key with Multiple S/N Lines | 274 |
| Figure 5-69: Regional Settings Screen | 276 |
| Figure 5-70: Maintenance Actions Screen | 277 |
| Figure 5-71: Maintenance Actions Screen | 278 |
| Figure 5-72: Maintenance Actions Screen | 279 |
| Figure 5-73: Configuration File Screen | 280 |
| Figure 5-74: Graphical Display of the Hardware | 282 |
| Figure 5-75: Trunk and Channel Status Screen | 285 |
| Figure 5-76: Basic Information Screen | 285 |
| Figure 5-77: Basic Information Screen | 286 |
| Figure 5-78: Module Status Indicators | 287 |
| Figure 5-79: Monitoring Ethernet, Power, Fan and Dry Contacts | 288 |
| Figure 5-80: Active Alarms Screen | 289 |
| Figure 5-81: Ethernet Port Information Screen | 289 |
| Figure 5-82: Assigning a Port Name | 290 |
| Figure 5-83: Remove Module Button Appears after Clicking Module Name | 291 |
| Figure 5-84: Module Removal Confirmation Message Box | 291 |
| Figure 5-85: Removed Module | 291 |

| | |
|--|-----|
| Figure 5-86: Insert Module Button after Clicking Module's Name | 292 |
| Figure 5-87: Log Off Confirmation Box..... | 292 |
| Figure 7-1: Call Flow for One-Stage Dialing..... | 388 |
| Figure 7-2: Call Flow for Two-Stage Dialing..... | 390 |
| Figure 7-3: Call Flow for Collecting Digits Mode | 393 |
| Figure 7-4: SIP Call Flow..... | 406 |
| Figure 7-5: Assigning Phone Numbers | 411 |
| Figure 7-6: Tel to IP Routing Screen..... | 412 |
| Figure 7-7: Endpoint Phone Number Screen | 413 |
| Figure 7-8: Automatic Dialing Screen..... | 413 |
| Figure 7-9: Tel to IP Routing Screen..... | 414 |
| Figure 7-10: Endpoint Phone Number Screen | 414 |
| Figure 7-11: Automatic Dialing Screen..... | 414 |
| Figure 7-12: Tel to IP Routing Screen..... | 414 |
| Figure 8-1: VLAN Settings Screen - Example | 435 |
| Figure 8-2: IP Settings Screen - Example | 436 |
| Figure 8-3: IP Routing Table - Example | 436 |
| Figure 10-1: Simple Conferencing SIP Call Flow | 450 |
| Figure 10-2: Advanced Conferencing SIP Call Flow | 453 |
| Figure 10-3: Modifying a Conference - SIP Call Flow | 454 |
| Figure 10-4: Applying Media Services on a Conference -- SIP Call Flow..... | 455 |
| Figure 10-5: Terminating a Conference -- SIP Call Flow | 456 |
| Figure 10-6: Conference Call Flow Example..... | 457 |
| Figure 10-7: MSCML Architecture..... | 465 |
| Figure 10-8: Announcement Call Flow | 472 |
| Figure 10-9: Direct Connection (Example)..... | 475 |
| Figure 10-10: Using an Application Server (Example) | 476 |
| Figure 14-1: Connection Module (CM) | 488 |
| Figure 14-2: iPMX Module..... | 488 |
| Figure 14-3: Hard Drive Module (HDMX) | 488 |
| Figure 14-4: Mediant 1000 Front Panel..... | 489 |
| Figure 14-5: Inserting CM Module..... | 489 |
| Figure 14-6: Mediant 1000 Rear Panel | 490 |
| Figure 14-7: Mediant 1000 with Cover Plates Removed..... | 490 |
| Figure 14-8: Mediant 1000 with Cutter Tool..... | 491 |
| Figure 14-9: Inserting iPMX Module..... | 491 |
| Figure 14-10: Inserting HDMX Module..... | 492 |
| Figure 15-1: Mediant 1000 Front Panel OSN Server Connections | 496 |
| Figure 15-2: Disk 1 of Redhat Partner Installation | 498 |
| Figure 15-3: Images Folder | 498 |
| Figure 15-4: ISO Screen..... | 499 |
| Figure 15-5: Selecting Extract Option | 500 |
| Figure 15-6: Extracting Files to Partner Install Folder..... | 500 |
| Figure 15-7: ISO-Extract Screen | 501 |
| Figure 15-8: Text Edit Screen | 501 |
| Figure 15-9: Deleting CFG | 503 |
| Figure 15-10: File Add..... | 503 |
| Figure 15-11: ISO Open Function | 504 |
| Figure 15-12: Choose a Language..... | 505 |
| Figure 15-13: WinISO - Actions Screen | 507 |
| Figure 15-14: Create ISO from CD-ROM | 508 |
| Figure 15-15: Creating .iso File | 508 |
| Figure 15-16: Partner Install Folder..... | 509 |
| Figure 15-17: Extract isolinux.cfg | 509 |
| Figure 15-18: Extracting Files to Partner Install Folder..... | 509 |
| Figure 15-19: Deleting CFG | 512 |
| Figure 15-20: File Add..... | 512 |

| | |
|---|-----|
| Figure 15-21: ISO Open Function | 513 |
| Figure 15-22: WinISO - Actions Screen | 516 |
| Figure 15-23: Create ISO from CD-ROM | 517 |
| Figure 15-24: Creating .iso File | 517 |
| Figure 15-25: Partner Install Folder..... | 518 |
| Figure 15-26: Extract isolinux.cfg File | 518 |
| Figure 15-27: Extracting Files to Partner Install Folder..... | 518 |
| Figure 15-28: isolinux.cfg File | 520 |
| Figure 15-29: Deleting CFG File | 522 |
| Figure 15-30: Add CFG File | 522 |
| Figure 15-31: Partner Install Folder..... | 523 |
| Figure 15-32: Save boot.iso | 523 |

List of Tables

| | |
|---|-----|
| Table 2-1: Mediant 1000 Front View Component Descriptions..... | 22 |
| Table 2-2: Analog I/O Modules LEDs Description..... | 27 |
| Table 2-3: Digital I/O Modules LED Description..... | 28 |
| Table 2-4: Power Supply Module LED Description..... | 28 |
| Table 2-5: CPU Module LEDs Description..... | 28 |
| Table 2-6: Mediant 1000 Rear Panel Connectors Component Descriptions..... | 29 |
| Table 3-1: Mediant 1000 Lifeline Setup Component Descriptions..... | 38 |
| Table 3-2: Dry Contact Operational Description..... | 40 |
| Table 4-1: Default Networking Parameters..... | 47 |
| Table 4-2: Configuration Parameters Available via the Voice Menu..... | 53 |
| Table 5-1: Available Access Levels and their Privileges..... | 58 |
| Table 5-2: Default Attributes for the Accounts..... | 58 |
| Table 5-3: Customizable Logo ini File Parameters..... | 67 |
| Table 5-4: Web Appearance Customizable ini File Parameters..... | 67 |
| Table 5-5: Customizable Logo ini File Parameters..... | 69 |
| Table 5-6: Web Appearance Customizable ini File Parameters..... | 69 |
| Table 5-7: User-Defined Welcome Message ini File Parameter..... | 70 |
| Table 5-8: General Parameters (Protocol Definition)..... | 73 |
| Table 5-9: Proxy & Registration Parameters..... | 85 |
| Table 5-10: Supported Coders..... | 96 |
| Table 5-11: DTMF and Dialing Parameters..... | 99 |
| Table 5-12: General Parameters (Advanced Parameters)..... | 104 |
| Table 5-13: Supplementary Services Parameters..... | 114 |
| Table 5-14: Metering Tones Parameters..... | 119 |
| Table 5-15: Keypad Features Parameters..... | 122 |
| Table 5-16: Stand-Alone Survivability Parameters..... | 124 |
| Table 5-17: Number Manipulation Parameters..... | 127 |
| Table 5-18: Dialing Plan Notations..... | 128 |
| Table 5-19: NPI/TON Values for ISDN ETSI..... | 129 |
| Table 5-20: Phone-Context Parameters..... | 131 |
| Table 5-21: General Parameters (Routing Tables)..... | 133 |
| Table 5-22: Tel to IP Routing Table..... | 137 |
| Table 5-23: IP to Trunk Group Routing Table..... | 139 |
| Table 5-24: Trunk Group Table..... | 151 |
| Table 5-25: Hunt Group Settings Parameters..... | 153 |
| Table 5-26: Call Forward Table..... | 158 |
| Table 5-27: Digital Gateway Parameters..... | 162 |
| Table 5-28: RADIUS Parameters..... | 167 |
| Table 5-29: FXO Parameters..... | 169 |
| Table 5-30: Voice Mail Parameters..... | 173 |
| Table 5-31: IPmedia Configuration Parameters..... | 176 |
| Table 5-32: Network Settings -- IP Settings Parameters..... | 179 |
| Table 5-33: Network Settings, Application Settings Parameters..... | 183 |
| Table 5-34: Network Settings -- NFS Settings Parameters..... | 186 |
| Table 5-35: IP Routing Table Column Description..... | 187 |
| Table 5-36: Network Settings -- VLAN Settings Parameters..... | 189 |
| Table 5-37: Media Settings, Voice Settings Parameters..... | 191 |
| Table 5-38: Media Settings -- Fax/Modem/CID Parameters..... | 195 |
| Table 5-39: Media Settings, RTP / RTCP Parameters..... | 199 |
| Table 5-40: Media Server Parameters..... | 203 |
| Table 5-41: Media Settings, Hook-Flash Settings Parameters..... | 204 |
| Table 5-42: Media Settings - General Media Settings Parameters..... | 205 |
| Table 5-43: E1/T1/J1 Configuration Parameters..... | 209 |
| Table 5-44: CAS State Machine Parameters..... | 220 |

| | |
|--|-----|
| Table 5-45: TDM Bus Settings Parameters..... | 222 |
| Table 5-46: Internal Firewall Parameters | 227 |
| Table 5-47: General Security Settings Parameters..... | 233 |
| Table 5-48: IPSec SPD Table Configuration Parameters | 237 |
| Table 5-49: Default IKE Second Phase Proposals | 238 |
| Table 5-50: IKE Table Configuration Parameters | 241 |
| Table 5-51: Default IKE First Phase Proposals..... | 242 |
| Table 5-52: Management Settings Parameters..... | 244 |
| Table 5-53: SNMP Trap Destinations Table Parameters..... | 247 |
| Table 5-54: SNMP Community Strings Parameters..... | 249 |
| Table 5-55: SNMP V3 Users Parameters | 250 |
| Table 5-56: IP Connectivity Parameters..... | 252 |
| Table 5-57: Call Counters Description | 254 |
| Table 5-58: Call Routing Status Parameters..... | 256 |
| Table 5-59: SAS Registered Users Parameters | 257 |
| Table 5-60: Ethernet Port Information Parameters | 260 |
| Table 5-61: Auxiliary Files Descriptions | 269 |
| Table 5-62: Description of the Areas of the Home Page..... | 283 |
| Table 5-63: Trunk and FXO/FXS Channel Status Color Indicators | 284 |
| Table 5-64: Trunk's Channel Status Color Indicators..... | 286 |
| Table 5-65: Description of the Module Status Indicators | 287 |
| Table 5-66: Description of Ethernet Ports, Dry Contacts, Power Supply, and Fan Tray Indicators.... | 288 |
| Table 5-67: | 291 |
| Table 6-1: Networking Parameters..... | 299 |
| Table 6-2: System Parameters..... | 308 |
| Table 6-3: Web and Telnet Parameters | 315 |
| Table 6-4: Security Parameters..... | 318 |
| Table 6-5: RADIUS Parameter | 320 |
| Table 6-6: SNMP Parameters | 321 |
| Table 6-7: SIP Configuration Parameters | 323 |
| Table 6-8: IPmedia Configuration Parameters | 337 |
| Table 6-9: Voice Mail Configuration Parameters | 338 |
| Table 6-10: PSTN Parameters | 340 |
| Table 6-11: ISDN and CAS Interworking-Related Parameters | 343 |
| Table 6-12: Analog Telephony Parameters..... | 350 |
| Table 6-13: Number Manipulation and Routing Parameters..... | 359 |
| Table 6-14: Channel Parameters | 372 |
| Table 6-15: Configuration Files Parameters..... | 378 |
| Table 7-1: Supported X-Detect Event Types..... | 395 |
| Table 7-2: Supported CDR Fields | 400 |
| Table 7-3: Supported RADIUS Attributes..... | 402 |
| Table 8-1: Traffic / Network Types and Priority | 432 |
| Table 8-2: Example of VLAN and Multiple IPs Configuration..... | 434 |
| Table 9-1: Mapping of ISDN Release Reason to SIP Response | 441 |
| Table 9-2: Mapping of SIP Response to ISDN Release Reason | 443 |
| Table 9-3: Calling Name (Display) | 448 |
| Table 9-4: Redirect Number | 448 |
| Table 12-1: Mediant 1000 Functional Specifications | 481 |
| Table 13-1: Supplied Software Package | 485 |

Notice

This document describes the AudioCodes Mediant 1000 Voice-over-IP (VoIP) SIP media gateway.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered Technical Support customers at <http://www.audiocodes.com> under Support / Product Documentation.

© Copyright 2007 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: Aug-30-2007

Date Printed: Sep-02-2007



Tip: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press the **ALT** and **←** keys

Trademarks

AC logo, Ardito, AudioCoded, AudioCodes, AudioCodes logo, CTI², CTI Squared, InTouch, IPmedia, Mediant, MediaPack, MP-MLQ, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, 3GX, TrunkPack, VoicePacketizer, VoIPerfect, What's Inside Matters, Your Gateway To VoIP, are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used. Only industry-standard terms are used throughout this manual. Hexadecimal notation is indicated by 0x preceding the number.

Related Documentation

| Document # | Manual Name |
|---|---|
| LTRT-523xx (where xx is the document version) | SIP Series Reference Manual |
| LTRT-831xx | Mediant 1000 SIP Release Notes |
| LTRT-835xx | Mediant 1000 MEGACO-SIP Fast Track Guide |
| LTRT-665xx | CPE SIP Configuration Guide for IP Voice Mail |



Warning: Ensure that you connect FXS ports to analog telephone or to PBX-trunk lines only and FXO ports to CO/PBX lines only.



Warning: Disconnect the gateway from the mains and from the Telephone Network Voltage (TNV) before servicing.



Warning: To protect against electrical shock and fire, use a 26 AWG min wire to connect FXO ports to the Public Switching Telephone Network (PSTN).



Warning: The FXO port is considered to be TNV-3. FXS ports are considered to be TNV-2.



Note: Throughout this manual, unless otherwise specified, the term *gateway* refers to the Mediant 1000.



Note: The terms *IP-to-Tel* and *Tel-to-IP* refer to the direction of the call relative to the AudioCodes device: *IP-to-Tel* refers to calls received from the IP network and destined to the PSTN (i.e., telephone connected directly or indirectly to the device); *Tel-to-IP* refers to calls received from the PSTN and destined for the IP network.



Note: Throughout this manual, the term 'Trunk' is used synonymously with 'Hunt'. Trunk typically refers to digital modules, while Hunt typically refers to analog modules.

1 Overview

The AudioCodes Mediant 1000 is a best-of-breed Voice-over-IP (VoIP) SIP media gateway, using field-proven, market-leading technology, implementing analog and digital cutting-edge technology. The Mediant 1000 is designed to seamlessly interface between TDM and IP networks, providing superior voice quality and optimized packet voice streaming (voice, fax, and data traffic) over IP networks.

The Mediant 1000 is best suited for small-to-medium size (SME) enterprises, branch offices, or for residential media gateway solutions. The Mediant 1000 is a highly scalable and modular system that matches the density requirements for smaller environments, while meeting service providers' demands for growth.

The Mediant 1000 is ideal for connecting an enterprise's legacy telephones, fax machines and PBX systems to IP-based telephony networks, as well as for seamless connection of IP-based PBX architecture to the PSTN. In addition to operating as a pure media gateway, the Mediant 1000 open platform extends its flexibility with additional deployment options to host partner applications, known as the Open Solutions Network (OSN) Server for supporting third-party VoIP applications such as IP-PBX, Pre-Paid, and IP-PBX redundancy.

The Mediant 1000 also provides conferencing services over VoIP networks. This is supported by an optional Media Process module (MPM) that can be housed in the Mediant 1000 chassis.

The Mediant 1000 is fully interoperable with multiple vendor gateways, softswitches, SIP servers, gatekeepers, proxy servers, IP phones, session border controllers, and firewalls. The Mediant 1000 is designed to meet NEBS Level 3 (Bellcore) and regulatory approval (including Safety, EMC, and Telecom for USA, EU and other countries).

Intelligently packaged in a stackable 1U chassis, the Mediant 1000 gateways are very compact devices that can be mounted as desk-top units, on the wall, or in standard 19-inch racks. The Mediant 1000 is provided with two integral mounting brackets for facilitating rack installation.

Mediant 1000 units are equipped with two 10/100 Base-TX Ethernet ports for connection to the IP network. The second Ethernet port is used for 1+1 Ethernet redundancy.

The Mediant 1000 supports mixed digital and analog interface configurations:

- The Mediant 1000 digital interface supports multiples of 1, 2, or 4 E1/T1/J1 spans used for connecting the PSTN or PBX to the IP network. The digital modules provide RJ-48 ports. The digital module can be configured as regular E1/T1/J1 interfaces, and with up to 1 or 2 paired spans acting as Lifeline telephone interfaces for switching to the PSTN in case of power failure or network problems.
- The Mediant 1000 analog interface supports up to 24 analog ports (four ports per module) in various Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) configurations, supporting up to 24 simultaneous VoIP calls. Each analog module comprises four analog RJ-11 ports. The FXO module can be used to connect analog lines of an enterprise's PBX or of the PSTN to the IP network. The FXS module can be used to connect legacy telephones, fax machines, and modems to the IP network. Optionally, the FXS module can be connected to the external trunk lines of a PBX. When deployed with a combination of FXO and FXS modules, the Mediant 1000 can be used as a PBX for Small Office Home Office (SOHO) users, and businesses not equipped with a PBX.

The Mediant 1000 has enhanced hardware and software capabilities to ease its installation and to help maintain voice quality. If the measured voice quality falls beneath a pre-configured value, or the path to the destination is disconnected, the Mediant 1000 can assure voice connectivity by falling back to the PSTN. In the event of network problems or power failures, calls can be routed back to the PSTN without requiring routing modifications in the PBX. Further reliability is provided by dual Ethernet ports and optional dual AC power supply.

The Mediant 1000 supports various ISDN PRI protocols such as EuroISDN, North American NI2, Lucent™ 4/5ESS, Nortel™ DMS100 and others. In addition, it supports different variants of CAS protocols for E1 and T1 spans, including MFC R2, E&M immediate start, E&M delay dial / start, loop start and ground start.

The Mediant 1000 provides a user-friendly embedded HTTP-based Web server for remote configuration and management using a standard Web browser (such as Microsoft™ Internet Explorer™ or Netscape™ Navigator™), from anywhere in the world with IP connectivity to the device.

1.1 SIP Overview

Session Initialization Protocol (SIP) is an application-layer control (signaling) protocol used on the gateway for creating, modifying, and terminating sessions with one or more participants. These sessions can include Internet telephone calls, media announcements, and conferences.

SIP invitations are used to create sessions and carry session descriptions that enable participants to agree on a set of compatible media types. SIP uses elements called Proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies and provide features to users.

SIP also provides a registration function that enables users to upload their current locations for use by Proxy servers. SIP implemented in the gateway, complies with the Internet Engineering Task Force (IETF) RFC 3261 (refer to <http://www.ietf.org>.)

2 Physical Description

Designed to meet Network Equipment Building System (NEBS) Level 3, the Mediant 1000 is a 19-inch industrial platform chassis, 1U high and 13.8 inch deep. The Mediant 1000 supports a scalable, modular architecture that includes various extractable modules: up to six analog modules, up to four digital modules, an optional Conference module, optional OSN Server modules, a single CPU module, a power supply module, and an optional fan try module.

This section provides a physical description of the following:

- Mediant 1000 front panel (refer to 'Mediant 1000 Front Panel' on page 21)
- Mediant 1000 rear panel (refer to 'Mediant 1000 Rear Panel' on page 29)

2.1 Mediant 1000 Front Panel

The figure below shows the front panel of the Mediant 1000.

Figure 2-1: Mediant 1000 Front View and CPU Enlargement

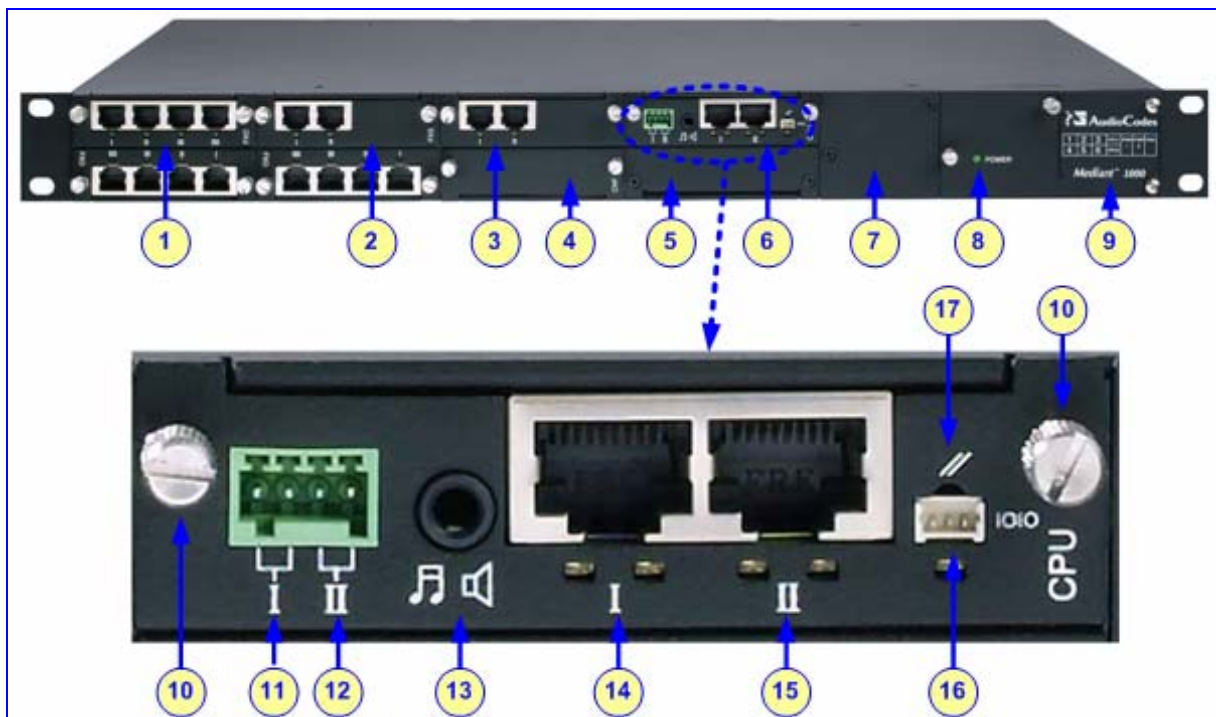


Table 2-1: Mediant 1000 Front View Component Descriptions

| Item # | Label | Component Description |
|------------------------------|------------------|--|
| Front View of Chassis | | |
| 1 | FXO | 4-port FXO (or FXO G) module. |
| 2 | FXS | 2-port FXS module. |
| 3 | TRUNKS | 2 RJ-48c ports digital module (E1/T1/J1). |
| 4 | MPM | Media Process module. |
| 5 | CPU | Spare CPU module slot or for OSN server where slot hosts Connection module (for OSN Server installation, refer to 'OSN Server Hardware Installation' on page 487). |
| 6 | CPU | Main CPU module. |
| 7 | Power 1 | Spare power supply slot. |
| 8 | Power 2 | Main power supply. |
| 9 | Schematic | Extractable fan tray. |
| Enlarged View of CPU | | |
| 10 | - | Locking screws (2). |
| 11 | I | Dry contact port (normally open). |
| 12 | II | Dry contact port (normally closed). |
| 13 | 🎵 | Audio IN/OUT (for paging and MOH (Music on Hold) functionalities). |
| 14 | I | 10/100 Base-TX Ethernet Port 1. |
| 15 | II | 10/100 Base-TX Ethernet Port 2. |
| 16 | I/O I/O | RS-232 port. |
| 17 | // | Reset button. |

The figure below illustrates the front layout of the Mediant 1000. There is also a schematic of the front layout on the front panel of the fan tray. To view your specific device's configuration using the Embedded Web Server, refer to 'Monitoring the Gateway (Home Page)' on page 282.

Figure 2-2: Mediant 1000 Front Layout

| | | | | | | |
|------------------------------|------------------------------|-------------------------------------|----------------|-------------------------|------------------------|---------------|
| Slot #1 I/O Module | Slot #2 I/O Module | Slot #3 I/O Module | Main CPU | Spare Power Supply Slot | Main Power Supply Unit | Fan Tray Unit |
| Slot #4 I/O Module | Slot #5 I/O Module | Slot #6 I/O or MPM Module | Spare CPU Slot | | | |



Note: The I/O modules must be housed in consecutive slots. In other words, if the Mediant 1000 houses three I/O modules, they must occupy slots 1, 2, and 3.

2.1.1 I/O Modules

The Mediant 1000 can house both analog and/or digital modules:

- **Analog modules:** the gateway supports up to six replaceable analog FXO and/or FXS modules. Each module contains four analog RJ-11 ports. Therefore, the gateway can support up to 24 analog ports (6 modules x 4 ports).

Figure 2-3: 4-Port FXS Analog Module



Figure 2-4: 4-Port FXO G (Ground Start) Analog Module



Figure 2-5: 4-Port FXO G (Ground Start) Analog Module



- **Digital modules:** the gateway supports up to four digital trunks (fully flexible, from a single up to four trunks per module). The digital modules are available in 1, 2, or 4 spans. If the power fails, a relay connects trunks 1 to 2, and 3 to 4 (in the same module) acting as a fallback for PSTN trunks.

Figure 2-6: Digital Module (e.g., 2 Spans)





Note: The standard FXO modules support outdoor and indoor (lightning protection) loop start signaling. For ground start signaling, the **FXO G** modules are required. These modules support loop and ground start, and only support indoor protection. (The FXS modules support both loop and ground start signaling.)
To enable ground start, use the *ini* file parameter GroundKeyDetection (refer to 'System Parameters' on page 308).

2.1.2 CPU Module

The CPU (Central Processing Unit) module, shown in the figure below, is located to the right of the six I/O analog/digital module slots.

Refer to the figure in 'Mediant 1000 Front Panel' on page 21 for a view of the CPU module's front panel ports and connectors, which are described in sequence from left to right in the following subsections.

Figure 2-7: CPU Module



2.1.2.1 Dry Contact Connector (Labeled I and II)

The Mediant 1000 provides dry contacts that can be connected to an external audible or visual alarm system (bell, siren, hooter, or light).

2.1.2.2 Audio IN/OUT1

The Audio IN/OUT port is indicated by the musical note and loudspeaker symbols (refer to the figure in 'Mediant 1000 Front Panel' on page 21). It is used for Music on Hold (IN) and paging (OUT).

2.1.2.3 10/100 Base-TX Ethernet Ports (Labeled I and II)

Two 10/100 Base-TX Ethernet ports provide a dual Ethernet redundancy scheme, protecting against failure (for example, a disconnection) of any cable or associated LAN switch port.

2.1.2.4 RS-232 Port (Labeled I0I0)

The RS-232 port is used to access the CLI (refer to 'Accessing the CLI' on page 53) and to receive error / notification messages (a 9-pin DB adapting cable is supplied).



Note: The RS-232 port is not intended for permanent connection.

2.1.2.5 Reset Button (Labeled //)

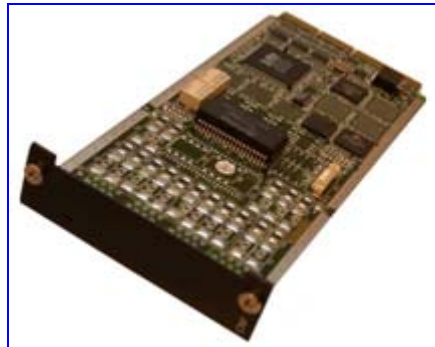
The Mediant 1000 Reset button is located directly above the RS-232 port. This button is used to reset the gateway and optionally, to restore the Mediant 1000 networking parameters to their factory default values (refer to 'Restoring and Backing up Configuration' on page 280).

To reset the system, take a pointed object and press in the Reset button.

2.1.3 Media Process Module (MPM)

The Mediant 1000 can optionally house a single Media Process module (MPM), as shown in the figure below. This module is used for media server support (i.e., conferencing). The module is installed in slot 6 of the chassis front panel. For a description of Mediant 1000 conferencing capabilities, refer to 'Media Server Capabilities' on page 449.

Figure 2-8: Media Process Module (MPM)

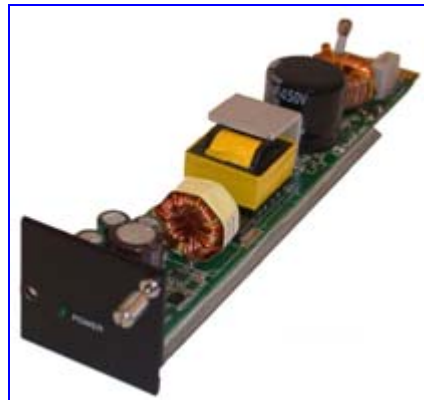


2.1.4 Power Supply Module (Labeled 1 and 2)

The Mediant 1000 features two extractable power supply units (Power 1 and Power 2), providing an AC power connector at the rear of each power unit. If both Power 1 and Power 2 units are used, the load is shared between them. This (optional) load-sharing feature enables failure protection / redundancy. When using this feature, you are advised to connect each power supply unit to a different AC supply circuit.

The front panel of the power supply unit provides a power supply LED that is lit green when the Mediant 1000 is powered up. If this LED does not light up, a power supply problem may be present.

Figure 2-9: Power Supply Module



2.1.5 Fan Tray Module

The Mediant 1000 components are cooled by a fan tray unit located to the extreme right of the front panel. The fan tray unit draws in air through a perforated grill at the right side of the chassis. The incoming air passes through a removable filter, whose honeycombed design prevents radio frequency (RF) interference. The clean air passes through the entire set of modules cooling each one, and then exits the Mediant 1000 via perforated vents on the left side of the chassis.

Figure 2-10: Fan Tray Module with Six Fans and an Air Filter



Blank panels are used to cover all unoccupied slots on the front and rear sides of the chassis. The blank panels are especially designed to assist optimal air flow within the chassis.

For replacing the fan tray unit, refer to 'Replacing the Air Filter' on page 45.



Note: It is imperative to cover all unoccupied slots in the front and rear panels of the chassis with blank panels to maintain internal airflow pressure.

2.1.6 Front Panel LEDs

The figure below shows the location of the front panel LEDs on the Mediant 1000. The LEDs are described in the tables below.

Figure 2-11: Location of Front Panel LEDs

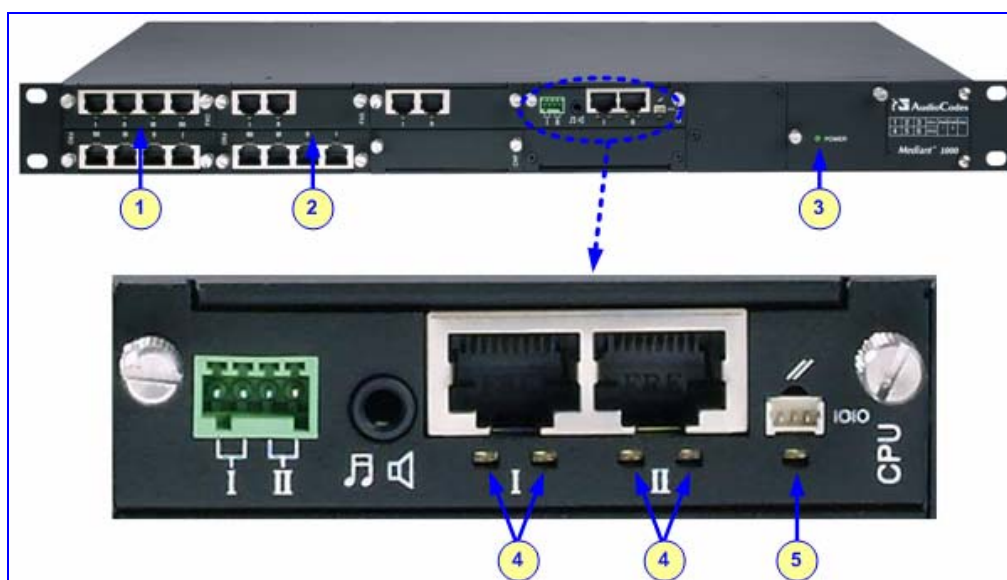


Table 2-2: Analog I/O Modules LEDs Description

| LED | Item # | Color | State | LED Indication |
|-------|--------|-------|----------|--|
| RJ-11 | 1 | Green | On | FXS phone is offhooked or FXO offhooks the line towards the PBX |
| | | | Blinking | FXS rings the extension line or the FXO detects a ring signal from the PBX |
| | | Red | On | Error (line is malfunctioning) |

Table 2-3: Digital I/O Modules LED Description

| LED | Item # | Color | State | LED Indication |
|--------|--------|-------|-------|---|
| RJ-48c | 2 | Green | On | Trunk is synchronized (normal operation) |
| | | Red | On | Loss due to any of the following 4 signals: <ul style="list-style-type: none"> ▪ LOS - Loss of Signal ▪ LOF - Loss of Frame ▪ AIS - Alarm Indication Signal (the Blue Alarm) ▪ RAI - Remote Alarm Indication (the Yellow Alarm) |
| | | -- | Off | Failure / disruption in the AC power supply or the power is currently not being supplied to the Mediant 1000 through the AC power supply entry. |

Table 2-4: Power Supply Module LED Description

| LED | Item # | Color | State | LED Indication |
|-------|--------|-------|-------|--|
| POWER | 3 | Green | On | The LED of each AC power supply is lit green when the power supply is operating correctly. |
| | | -- | Off | Failure / disruption in the AC supply, or the power is currently not being supplied to the Mediant 1000 through the AC power supply entry. |

Table 2-5: CPU Module LEDs Description

| LED | Item # | Color | State | LED Indication |
|-----------------------|---------------|--------|------------------------|-------------------------|
| Ethernet Ports I & II | 4 (Left LED) | Orange | Blinking | Activity. |
| | 4 (Right LED) | Green | On | Link OK. |
| | | Yellow | Blinking | Data is being received. |
| | | ---- | Off | No link. |
| General Purpose | 5 | Green | N/A. (Future support.) | |

2.2 Mediant 1000 Rear Panel


The Mediant 1000 rear panel provides the power connectors, as shown in the figure below.

Figure 2-12: Mediant 1000 Rear Connectors



The table below describes the Mediant 1000 rear panel components.

Table 2-6: Mediant 1000 Rear Panel Connectors Component Descriptions

| Item # | Label | Component Description |
|--------|---|-------------------------------------|
| 1 |  | Protective earthing screw. |
| 2 | ESD | Electrostatic Discharge (ESD) port. |
| 3 | 100-240V~1A | Dual AC Power Supply Entry. |



Note: The rear panel also provides module slots for housing OSN Server modules (viz., OSN Server and Hard Drive modules). For information on the OSN Server installation, refer to 'OSN Server Hardware Installation' on page [487](#)).

Reader's Notes

3 Installing the Mediant 1000

This section provides information on the hardware installation procedure for the Mediant 1000.



Caution Electrical Shock

The equipment must only be installed or serviced by qualified service personnel.

To install the Mediant 1000, perform the following installation steps in chronological order:

- Unpack the Mediant 1000 (refer to 'Unpacking' on page 31).
- Check the package contents (refer to 'Package Contents' on page 31).
- Mount the Mediant 1000 (refer to 'Mounting the Mediant 1000' on page 32).
- Cable the Mediant 1000 (refer to 'Cabling the Mediant 1000' on page 35).

After connecting the Mediant 1000 to the power source, the power LED on the front panel of the power supply unit is lit green. Any power supply malfunction results in the LED switching off (for details on the Mediant 1000 LEDs, refer to 'Front Panel LEDs' on page 27).

When you have completed the above installation steps, you are then ready to start configuring the gateway (refer to 'Web-based Management' on page 57).

3.1 Unpacking

Follow the procedure below for unpacking the received carton in which the Mediant 1000 is shipped.

➤ **To unpack the Mediant 1000, take these 6 steps:**

1. Open the carton and remove packing materials.
2. Remove the Mediant 1000 from the carton.
3. Check that there is no equipment damage.
4. Check, retain and process any documents.
5. Notify AudioCodes or your local supplier of any damage or discrepancies.
6. Retain any diskettes or CDs.

3.2 Package Contents

Ensure that in addition to the Mediant 1000, the package contains:

- One or two AC power cables.
- Four anti-slide bumpers for desktop installation option (supplied in a small plastic bag).
- CD (software and documentation).
- RS-232 DB9 adaptor cable, two meters in length (direct connection to PC).
- The Mediant 1000 Fast Track Guide.

3.3 Mounting the Mediant 1000

The Mediant 1000 offers the following mounting options:

- Desktop mounting (refer to 'Mounting Mediant 1000 on a Desktop' on page 32)
- Installed in a standard 19-inch rack (refer to 'Installing Mediant 1000 in a 19-inch Rack' on page 34)

3.3.1 Mounting Mediant 1000 on a Desktop

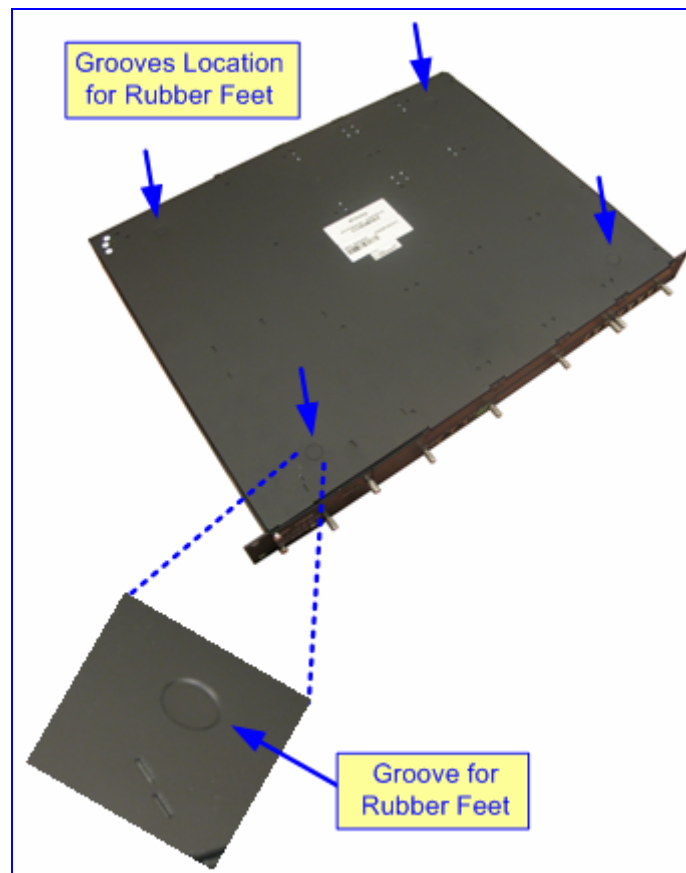
The Mediant 1000 can be mounted on a desktop by attaching the four anti-slide bumpers (supplied) to the underside of the Mediant 1000. Once you have attached these bumpers, simply place it on the desktop in the position you require.

Figure 3-1: Attached Rubber Foot on Underside of Chassis

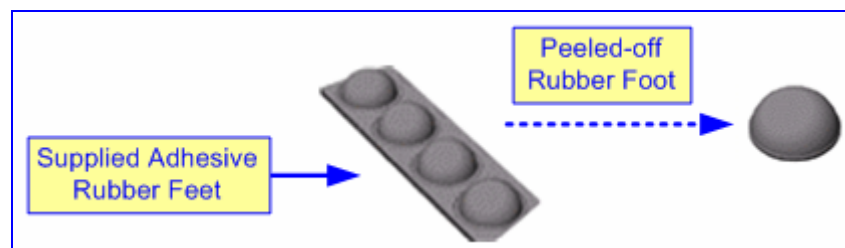


➤ **To stick the anti-slide rubber bumpers to the Mediant 1000, take these 4 steps:**

1. Flip the Mediant 1000 over so that its underside faces up.
2. Locate the four anti-slide grooves on the underside -- one on each of the four corners.

Figure 3-2: Location of Grooves for Rubber Feet

3. Peel off the adhesive, anti-slide rubber feet and stick one in each anti-slide groove.

Figure 3-3: Peeled-off Rubber Foot

4. Flip the Mediant 1000 over again so that it is resting on its underside.

3.3.2 Installing Mediant 1000 in a 19-inch Rack

The Mediant 1000 can be installed in a standard 19-inch rack by implementing one of the following methods:

- Placing it on a pre-installed shelf in the rack (recommended method)
- Attaching it directly to the rack's frame using the Mediant 1000 integral front mounting brackets and the user-adapted rear mounting brackets (not supplied). This method is required for racks that don't provide shelves.

Rack Mount Safety Instructions (UL)

When installing the chassis in a rack, be sure to implement the following Safety instructions recommended by Underwriters Laboratories:



- **Elevated Operating Ambient Temperature:** If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma}) specified by the manufacturer.
- **Reduced Air Flow:** Installation of the equipment in a rack should be such that the amount of air flow required for safe operation on the equipment is not compromised.
- **Mechanical Loading:** Mounting of the equipment in the rack should be such that a hazardous condition is not **achieved** due to uneven mechanical loading.
- **Circuit Overloading:** Consideration should be given to the connection of the equipment to the supply circuit **and** the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing:** Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips.)

➤ To mount the Mediant 1000 on a pre-installed shelf in the rack, take this step:

- Place the Mediant 1000 on a pre-installed shelf in the rack. It's recommended to attach the Mediant 1000 integral front mounting brackets to the rack's frame to prevent it from sliding off the shelf during cabling. Use standard 19-inch rack bolts (not provided) to fasten the front of the Mediant 1000 to the frame of the rack.

➤ **To install the Mediant 1000 in a rack without shelves, take these 2 steps:**

1. Position the Mediant 1000 in your 19-inch rack and align the *front and rear* (refer to note below) bracket holes to the holes (of your choosing) in the vertical tracks of the 19-inch rack.
2. Use standard 19-inch rack bolts (not provided) to fasten the brackets to the frame of the rack.



Note: If you are assembling the rear brackets by yourself, please note the following:

- The distance between the screws on each bracket is 28 mm.
- To attach the brackets, use 4-40 screws with a maximal box penetration length of 3.5 mm.

3.4 Cabling the Mediant 1000

This section describes Mediant 1000 cabling, which includes the following:

- Grounding Mediant 1000 (refer to 'Grounding Mediant 1000' on page 35)
- Connecting to the Ethernet network (refer to 'Connecting to the Ethernet Network' on page 36)
- Connecting to the FXS/FXO interfaces (refer to 'Connecting to FXS/FXO Interfaces' on page 36)
- Cabling the analog Lifeline telephone (refer to 'Cabling the Analog Lifeline Phone' on page 37)
- Connecting to digital trunks (refer to 'Connecting to Digital Trunks' on page 39)
- Cabling the digital Lifeline (refer to 'Cabling the Digital Lifeline' on page 40)
- Cabling the Dry Contact Relay Alarm System (refer to 'Cabling the Dry Contact Relay Alarm System' on page 40)
- Connecting the RS-232 interface to a PC (refer to 'Connecting the Mediant 1000 RS-232 Port to Your PC' on page 42)
- Connecting Mediant 1000 to the power supply (refer to 'Connecting Mediant 1000 to Power' on page 42)

3.4.1 Grounding Mediant 1000

The Mediant 1000 must be permanently grounded (earthed) using an equipment-earthing conductor.



Protective Earthing

The equipment is classified as Class I EN60950 and UL60950 and must be earthed at all times.

➤ **To ground the Mediant 1000, take these 2 steps:**

1. Connect an electrically earthed strap of 16 AWG wire (minimum) to the chassis earthing screw using the supplied washer.
2. Connect the strap to a protective earthing. This should be in accordance with the regulations enforced in the country of installation.

3.4.2 Connecting to the Ethernet Network

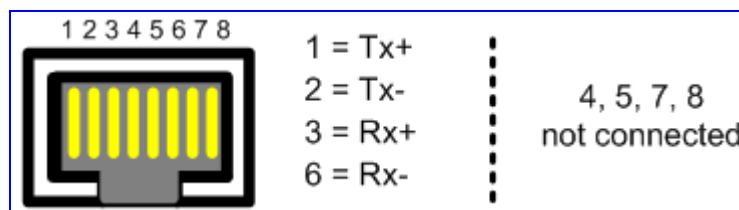
The Mediant 1000 CPU module provides two 10/100Base-TX RJ-45 ports for connection to the Ethernet network. The dual ports provide Ethernet redundancy. Follow the procedure below for connecting Mediant 1000 to the Ethernet network.

➤ **To connect Mediant 1000 directly to the Ethernet network:**

- Connect the first Ethernet port (labeled I), located on the CPU module of the Mediant 1000 front panel, directly to the network using a standard RJ-45 Ethernet cable. Connect the second Ethernet connection for optional redundancy / backup.

For the RJ-45 connector pinouts, refer to the figure below.

Figure 3-4: RJ-45 Connector Pinouts



When assigning an IP address to the Mediant 1000 using HTTP (in Step 1 in 'Assigning an IP Address Using HTTP' on page 50), you may be required to re-cable it differently.



Note: For Ethernet redundancy, it's recommended to connect each of the Ethernet ports to a different switch.

3.4.3 Connecting to FXS / FXO Interfaces

The procedure below describes the cabling for the Mediant 1000 FXS and FXO module analog interfaces.

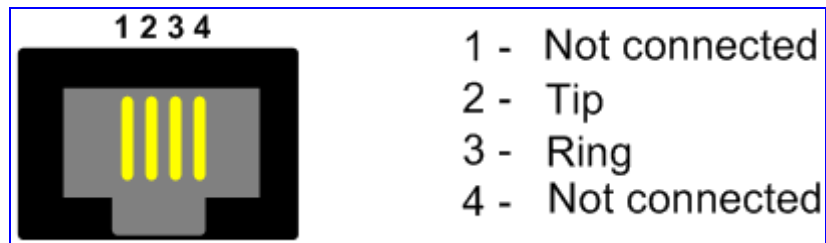


Warning: To protect against electrical shock and fire, use a 26 AWG min wire to connect FXO ports to the PSTN.

➤ **To connect the Mediant 1000 FXS / FXO interfaces:**

- Using the RJ-11 connectors (refer to the figure below for connector pinouts), connect the Mediant 1000 to the required telephone interfaces:
 - **FXS:** connect the Mediant 1000 FXS module's ports to fax machines, modems, or telephones.
 - **FXO:** connect the Mediant 1000 FXO module's ports to telephone exchange analog lines or PBX extensions.

Figure 3-5: RJ-11 Connector Pinouts



Note: Ensure that FXS and FXO ports are connected to the correct external devices, otherwise damage to the Mediant 1000 can occur.

3.4.4 Cabling the Analog Lifeline Phone

The gateway's FXS modules provide a Lifeline phone connection on Port 1.

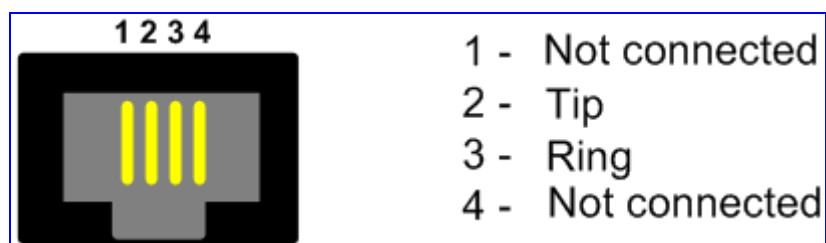


Note: Only the Mediant 1000 FXS modules support analog Lifeline.

The Lifeline provides a wired analog POTS phone connection to any PSTN or PBX FXS port when there is no power, or when the network connection fails. Therefore, you can use the Lifeline phone even when the Mediant 1000 is not powered on or not connected to the network.

The Lifeline splitter connects pins 1 and 4 to another source of an FXS port, and pins 2 and 3 to the POTS phone (refer to the Lifeline pinout in the figure below).

Figure 3-6: RJ-11 Connector Pinouts for FXS Lifeline



The use of the Lifeline on network failure can be disabled using the LifeLineType *ini* file parameter (described in 'Analog Telephony Parameters' on page 350).

➤ **To cable the Mediant 1000 FXS module's Lifeline, take these 3 steps:**

1. Connect the Lifeline Splitter (supplied) to Port 1 on the Mediant 1000 FXS module.
2. Connect the Lifeline phone to Port A on the Lifeline Splitter.
3. Connect an analog PSTN line to Port B on the Lifeline Splitter.

Figure 3-7: Mediant 1000 Lifeline Setup

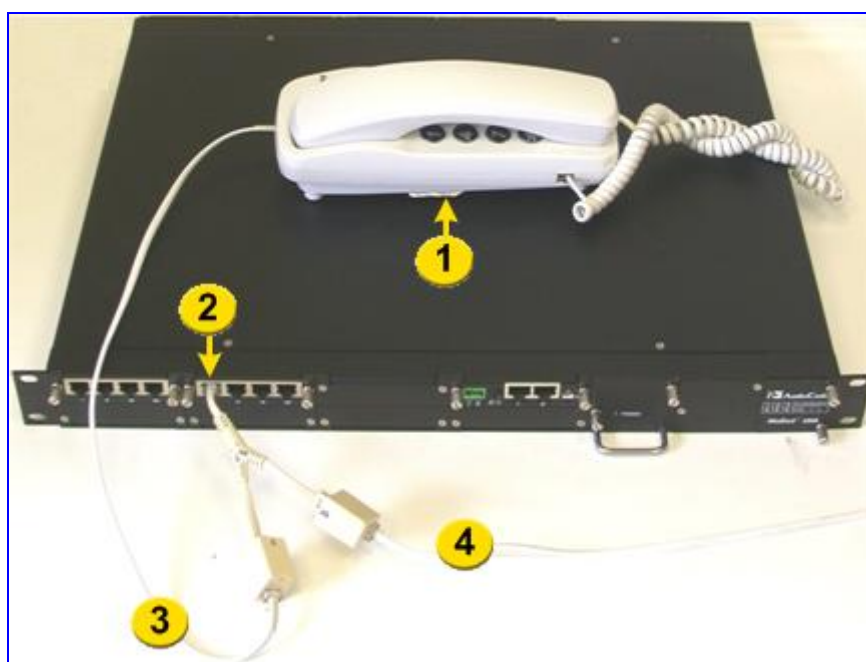


Table 3-1: Mediant 1000 Lifeline Setup Component Descriptions

| Item # | Component Description |
|--------|--|
| 1 | Lifeline phone. |
| 2 | Lifeline connected to FXS module Port 1. |
| 3 | Splitter (A) to Lifeline phone. |
| 4 | Splitter (B) to PSTN or PBX extension analog line. |

3.4.5 Connecting to Digital Trunks

The procedure below describes the cabling for the Mediant 1000 digital module interfaces (i.e., E1/T1 trunks). This also includes cabling for PSTN Fallback, which allows Trunks to connect to the PSTN during a power outage (i.e., no communication with IP network).



Warning: To protect against electrical shock and fire, use a 26 AWG min wire to connect T1 or E1 ports to the PSTN.

➤ **To connect the digital trunk interfaces:**

1. Connect the E1/T1 trunk cables to the ports on the Mediant 1000 digital I/O module(s).
2. Connect the other ends of the trunk cables to your PBX/PSTN switch.

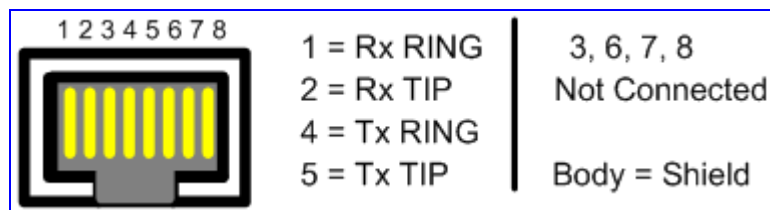
The digital trunks can be connected in such a way to support PSTN Fallback in case of power outage.

➤ **To connect the digital trunk interfaces for PSTN Fallback:**

- For a 1+1 or 2+2 Fallback option, connect Trunks 1 and 3 to your PBX, and Trunks 2 and 4 to the PSTN. If the power fails, a relay connects Trunks 1 to 2, and 3 to 4 (in the same module) acting as a Fallback for PSTN trunks.

RJ-48c trunk connectors are wired according to the figure below.

Figure 3-8: RJ-48c Connector Pinouts



3.4.6 Cabling the Digital Lifeline

The Mediant 1000 gateway containing either one or two digital modules, each with 1 or 2 pairs of spans can provide a “lifeline” telephone link. In the event of a power failure, a relay connects trunk 1 to 2, and / or 3 to 4 in the same module. The link is provided by the closing of a metallic switch inside the module so that the trunk from the PBX is routed from the module to the PSTN.



Note: The Lifeline feature can only be supported between ports on the same digital module.

Figure 3-9: Mediant 1000 Digital Lifeline Cabling (e.g., Trunks 1 and 2)



3.4.7 Cabling the Dry Contact Relay Alarm System

The dry contact ports I and II located on the gateway's CPU module (refer to 'Setting up a Dry Contact Relay Alarm System' on page 40), allows you to connect the gateway to an external audible or visual alarm system. The table below describes the operational status of these dry contact ports.

Table 3-2: Dry Contact Operational Description

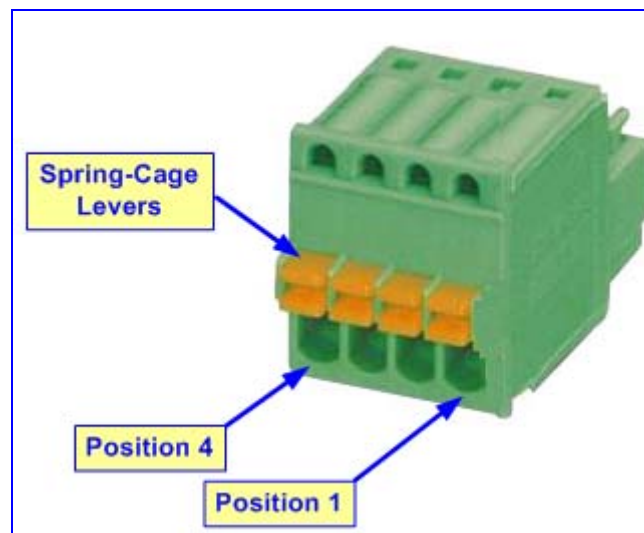
| Port | Normal State | Alarm Severity State |
|------|---|---|
| I | During normal operation, the dry contact is open. | If a Major alarm is generated, the dry contact closes. |
| II | During normal operation, the dry contact is open. | If a Critical alarm is generated, the dry contact closes. |

You can view a detailed description of these alarms by accessing the Active Alarms Table (refer to 'Viewing the Active Alarms Table' on page 288) in the gateway's embedded Web server.

The external alarm system is connected to the Mediant 1000 gateway's dry contact connector on the CPU module, using the supplied dry contact wires' mate (refer to the figure below). The mate provides four spring-cage terminal block connector labeled 4, 3, 2 and 1 (from left to right). These connections correspond to the four pins of the dry contact connector on the CPU module.

You need to supply your own wiring (for connecting to the mate's spring-cage connections) as well as a visual and/or audible alarm system attached at the other end of the wires. The dry contact connector suites wire sizes in the range 20 to 28 AWG. In addition, the dry contact system can receive a current of up to 1.5 A.

Figure 3-10: Dry Contact Wires' Mate



Note: The dry contact alarm provided on the CPU card should be connected only to SELV (Safety Extra-Low Voltage) non-energy hazard sources (Class 2) as per UL 60950 and EN 60950.

➤ **To set up a dry contact system, take these 2 steps:**

1. Insert two wires into the mate's spring-cage wire connectors in position 4 and 3 for the gateway's dry contact port I, and two wires in position 2 and 1 (for the gateway's dry contact port II), by performing the following:
 - a. With a sharp, pointed object, press the position's corresponding orange button; the cage of the connection opens.
 - b. Insert the wire into the connector and then release the orange button; the cage closes, securing the wire in place.
2. Connect the other ends of the dry contact wiring to the alerts system (alarm, siren, or light) according to your preferences and requirements.

3.4.8 Connecting the Mediant 1000 RS-232 Port to a PC

The Mediant 1000 RS-232 port is used to access the CLI (refer to 'Accessing the CLI' on page 53) and to receive error / notification messages.

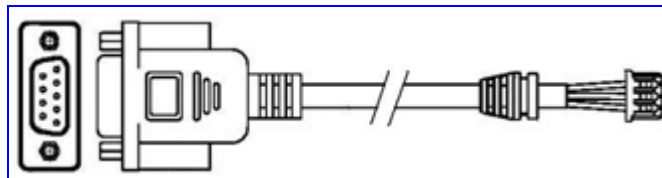
Follow the procedure below to connect the Mediant 1000 serial (RS-232) interface to a PC.

➤ **To connect Mediant 1000 to a PC, take these 2 steps:**

1. Connect the connector (refer to the figure below), on one end of the crossover RS-232 cable, to the Mediant 1000 RS-232 port (Labeled **I010**).
2. Connect the DB-9 connector at the other end of the cable, to either the COM1 or COM2 RS-232 communication port on your PC.

For information on establishing a serial communications link with the Mediant 1000, refer to Establishing a Serial Communications Link with the Mediant 1000.

Figure 3-11: RS-232 Cable Adaptor



3.4.9 Connecting Mediant 1000 to Power

The Mediant 1000 can house up to two extractable power supply units (Power 1 and Power 2), each providing an AC power connector on the Mediant 1000 rear panel. For detailed information on the power supply module, refer to 'Power Supply Module' on page 25.

➤ **To connect Mediant 1000 to the power supply:**

- On the Mediant 1000 rear panel, connect the left (active) 100-240V~50-60 Hz power socket to a standard electrical outlet using the supplied AC power cord.



Note: If both power units are used (for load sharing -- failure protection / redundancy), ensure that you connect each power supply unit to a different AC supply circuit.

3.5 Maintenance

This section describes the following maintenance operations:

- Replacing modules (refer to 'Replacing Modules' on page 43)
- Inserting additional modules (refer to 'Inserting Modules into Previously Empty Slots' on page 44)
- Replacing the Fan Tray unit (refer to 'Replacing the Air Filter' on page 45)

3.5.1 Replacing Modules

The Mediant 1000 I/O modules are hot-swappable (except for the OSN Server modules -- refer to 'OSN Server Hardware Installation' on page 487). The replacement of Mediant 1000 communication modules (i.e., digital, FXS, and FXO) is performed using the Mediant 1000 embedded Web server. Once you have 'removed' the module using the Web server, you need to physical remove and then insert a new module. Once the new module is physically inserted, you then need to 'insert' it using the Web server.

**Warnings:**

- Replace damaged modules with the identical module type and in the exact module slot. For example, a module with two digital spans in Slot 1 must be replaced with a module with two digital spans in Slot 1.
- When only one module is available, removal of the module causes the device to reset.

➤ **To replace Mediant 1000 modules, take these 4 steps:**

1. Remove the module using the embedded Web server (refer to 'Replacing Modules' on page 290).
2. Physical remove the module from the Mediant 1000 front-panel slot, by performing the following:
 - a. Using a flathead screwdriver, loosen the module's two mounting screws.
 - b. Gently extract the module from the slot.
3. Physical insert the new module into the same slot from where the module that you are replacing resided, by performing the following:
 - a. Insert the module into the empty slot, with the plain side of the Printed Circuit Board (PCB) facing up. Make sure the PCB slides into the slot rails by aligning the module with the rails in the slot.
 - b. Push the module into the slot and press on it firmly to ensure it has been fully inserted.
 - c. Using a flathead screwdriver, tighten the module's mounting pins.
4. Insert the module using the embedded Web server (refer to 'Replacing Modules' on page 290).

3.5.2 Inserting Modules into Previously Empty Slots

The procedure below describes how to add additional modules (i.e., digital, and FXS and FXO analog) to previously empty module slots in the gateway.



Warning: Ensure that you switch off the power to the gateway before adding a module to a previously empty slot.



Note: The standard FXO module supports outdoor and indoor (lightning protection) loop start signaling. For ground start signaling, the **FXO G** module is required. This module supports either loop or ground start (and only supports indoor protection). The FXS module supports both loop and ground start signaling. To enable ground start, use the *ini* file parameter GroundKeyDetection (refer to 'System Parameters' on page 308).

➤ **To install a module into a previously empty slot, take these 6 steps:**

1. Power off the Mediant 1000.
2. On the Mediant 1000 front panel, using a Phillips screwdriver remove the black metal cover plate protecting the module slot.
3. Insert the module into the empty slot, with the plain side of the Printed Circuit Board (PCB) facing up. Make sure the PCB slides into the slot rails by aligning the module with the rails in the slot.
4. Push the module into the slot and press on it firmly to ensure it has been fully inserted.
5. Using a flathead screwdriver, tighten the module's mounting pins.
6. Power on the Mediant 1000.

3.5.3 Replacing the Air Filter

The fan tray module includes a removable air filter (located within the fan assembly, immediately inside the perforated grill). The air filter should be replaced approximately every 90 days and should be checked weekly to ensure it is not saturated and that it does not require cleaning / replacement. You should clean the air filter no more than three times, after which the air filter should be replaced. Cleaning or replacing the air filter can be carried out while the system is fully functioning.

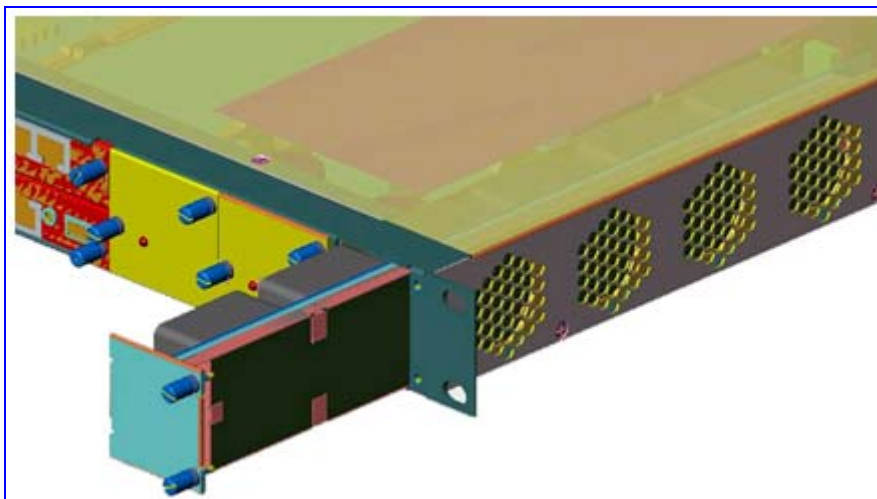
**Warnings:**

- When removing the Fan Tray unit while the power is on (or after it has recently been switched off), the blades may still be rotating at a high speed. Therefore, to avoid bodily harm ensure that you don't touch the fan blades.
- Before removing the Fan Tray unit for cleaning the air filter, prepare all the required equipment. It is imperative that the chassis does not remain without the fan tray unit for a long period of time. Ensure that you re-insert the Fan Tray unit (without the air filter) while you are cleaning the air filter, and then re-insert the air filter as soon as it is clean.

➤ **To clean / replace the air filter, take these 7 steps:**

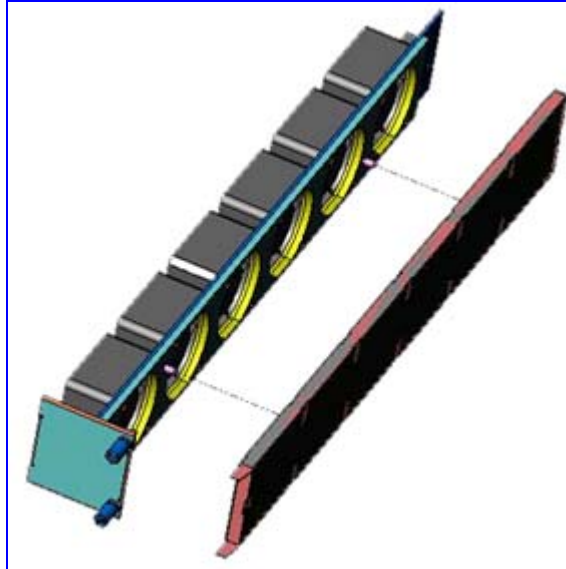
1. Release the two screws on the top right-hand corner and the bottom right-hand corner of the front panel of the fan tray unit.
2. Pull the fan tray unit outward. The figure below shows the fan tray unit slightly extracted.

Figure 3-12: Slightly Extracted Fan Try Unit



3. With your fingertips, grasp the steel frame of the air filter and separate it from the fan tray unit; you should be able to remove it relatively easily. The figure below shows the air filter extracted from the fan tray unit.

Figure 3-13: Fan Tray with Filter Removed



4. Take one of the following steps:
 - If you are cleaning the filter, use a vacuum cleaner (set to light suction) to remove dust particles from the filter.
 - Alternatively, if you are replacing the filter, discard the old air filter and replace it with an air filter purchased from AudioCodes.
5. Attach the (new / cleaned) air filter to the fan tray module; position the two holes on the filter over the pins on the fan tray.
6. Insert the fan tray unit into its slot, until the front panel is flush with the chassis plate.
7. Fasten the two screws on the top right-hand corner and the bottom right-hand corner of the front panel of the fan tray unit.

4 Getting Started

The gateway is supplied with default networking parameters (i.e., MAC and IP addresses, as listed in the table below) and with an application software (*cmp* file) residing on its flash memory (with factory default parameters).

Before you begin configuring the gateway, refer to 'Configuration Concepts' on page 47 for a description of the available gateway configuration methods. Using a preferred method, change the gateway's default IP address to correspond with your network environment (refer to 'Assigning an IP Address' on page 50).

For information on quickly setting up the gateway with basic parameters using a standard Web browser, refer to 'Configuring the Basic Parameters' on page 55.

Table 4-1: Default Networking Parameters

| Parameter | Default Value |
|----------------------------|---------------|
| IP Address | 10.1.10.10 |
| Subnet Mask | 255.255.0.0 |
| Default Gateway IP Address | 0.0.0.0 |

4.1 Configuration Concepts

You can deploy the gateway in a wide variety of applications enabled by its parameters and configuration files (e.g., Call Progress Tones). The parameters can be configured and configuration files can be loaded using the following tools:

- A standard Web browser (described in 'Web-based Management' on page 57).
- A configuration file referred to as the *ini* file. For information on how to use the *ini* file, refer to 'ini File Configuration' on page 293.
- An SNMP browser software (refer to the *SIP Series Reference Manual*).
- AudioCodes' Element Management System (refer to *AudioCodes' EMS User's Manual* or *EMS Product Description*).

To upgrade the gateway (i.e., load new software or configuration files), use the gateway's Embedded Web Server's Software Upgrade Wizard (refer to 'Software Upgrade Wizard' on page 262), or alternatively, use the BootP/TFTP configuration utility (refer to the *SIP Series Reference Manual*).

4.2 Startup Process

The startup process (illustrated in the following figure) begins when the gateway is reset (physically, using the Embedded Web Server, or using SNMP) and ends when the operational software is running. In the startup process, the network parameters, and software and configuration files are obtained.

After the gateway powers up or after it's physically reset, it broadcasts a BootRequest message to the network. If it receives a reply (from a BootP server), it changes its network parameters (IP address, subnet mask and default gateway address) to the values provided. If there is no reply from a BootP server and if DHCP is enabled (DHCPEnable = 1), the gateway initiates a standard DHCP procedure to configure its network parameters.

After changing the network parameters, the gateway attempts to load the *cmp* and various configuration files from the TFTP server's IP address, received from the BootP/DHCP servers. If a TFTP server's IP address isn't received, the gateway attempts to load the software (*cmp*) file and / or configuration files from a preconfigured TFTP server (refer to 'Automatic Update Mechanism' on page 266). Thus, the gateway can obtain its network parameters from BootP or DHCP servers, and its software and configuration files from a different TFTP server (preconfigured in the *ini* file).

If BootP/DHCP servers are not located or when the gateway is reset using the Embedded Web Server or SNMP, it retains its network parameters and attempts to load the software (*cmp*) file and / or configuration files from a preconfigured TFTP server. If a preconfigured TFTP server doesn't exist, the gateway operates using the existing software and configuration files loaded on its non-volatile memory.

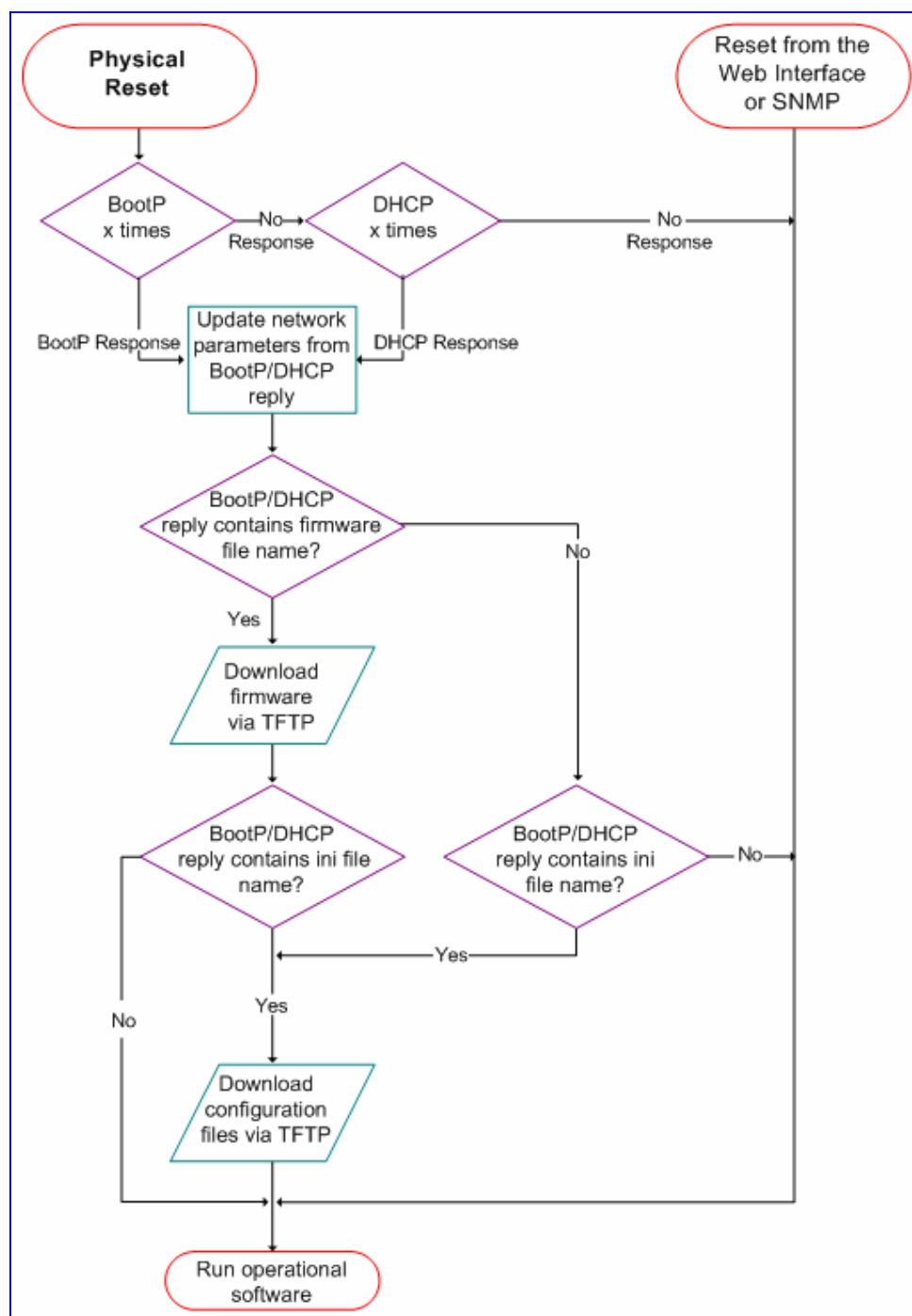
Note that after the operational software runs and if DHCP is configured, the gateway attempts to renew its lease with the DHCP server.



Notes:

- Though DHCP and BootP servers are very similar in operation, the DHCP server includes some differences that could prevent its operation with BootP clients. However, many DHCP servers such as Windows™ NT DHCP server are backward-compatible with BootP protocol and can be used for gateway configuration.
- By default, the duration between BootP/DHCP requests is one second (configured by the BootPDelay *ini* file parameter). The number of requests is three by default (configured by the BootPRetries *ini* file parameter). Both parameters can also be set using the BootP command line switches.

Figure 4-1: Startup Process



4.3 Assigning an IP Address

To assign the gateway an IP address, use one of the following methods:

- HTTP using a Web browser (refer to 'Assigning an IP Address Using HTTP' on page 50).
- BootP (refer to 'Assigning an IP Address Using BootP' on page 51).
- Voice Menu using a standard touch-tone telephone connected to one of the FXS analog ports (refer to Assigning an IP Address Using the Voice Menu Guidance on page 52). This method doesn't apply to FXO modules.
- Embedded Command Line Interface (CLI) accessed via RS-232 or Telnet (refer to 'Assigning an IP Address Using the CLI' on page 53).
- Dynamic Host Control Protocol (DHCP) (refer to the *SIP Series Reference Manual*).

Use the hardware Reset button at any time to restore the gateway's networking parameters to their factory default values (refer to 'Restoring Default Settings' on page 282).

4.3.1 Assigning an IP Address Using HTTP

You can assign the gateway an IP address using the gateway's HTTP-based Embedded Web Server.

➤ **To assign an IP address using HTTP, take these 9 steps:**

1. Disconnect the gateway from the network and reconnect it to a PC using one of the following two methods:
 - Connect the network interface on your PC to a port on a network hub / switch, using a standard Ethernet cable. Connect the gateway to another port on the same network hub / switch, using a second standard Ethernet cable.
 - Connect the network interface on your PC directly to the gateway, using an Ethernet cross-over cable.
2. Change your PC's IP address and subnet mask to correspond with the gateway's factory default IP address and subnet mask (for default IP addresses, refer to 'Getting Started' on page 47).
3. Access the gateway's Embedded Web Server (refer to 'Accessing the Embedded Web Server' on page 60).
4. Access the 'Quick Setup' screen by clicking the **Quick Setup** menu.
5. Define the gateway's 'IP Address', 'Subnet Mask', and 'Default Gateway IP Address' fields to correspond with your network IP settings.
6. Click the **Reset** button, and then at the prompt, click **OK**; the gateway applies the changes and restarts.
7. Disconnect your PC from the gateway or from the hub / switch (depending on the connection method used in Step 1).

8. Reconnect the gateway and your PC (if necessary) to the network.
9. Restore your PC's IP address and subnet mask to their original settings. If necessary, restart your PC and re-access the gateway via the Embedded Web Server with its newly assigned IP address.



Tip: Record and retain the IP address and subnet mask you assign the gateway. Do the same when defining new username or password. If the Embedded Web Server is unavailable (for example, if you've lost your username and password), use the BootP/TFTP (Trivial File Transfer Protocol) configuration utility to access the device, 'reflash' the load and reset the password (refer to the *SIP Series Reference Manual*). For detailed information on using a BootP/TFTP configuration utility to access the device).

4.3.2 Assigning an IP Address Using BootP

The procedure below describes how to assign the gateway an IP address using the supplied BootP application. For a detailed description on using AudioCodes' BootP application, refer to the *SIP Series Reference Manual*.



Note: BootP procedure can also be performed using any standard compatible BootP server.



Tip: You can also use BootP to load the auxiliary files to the gateway (refer to the *SIP Series Reference Manual*).

➤ To assign an IP address using BootP, take these 3 steps:

1. Open the BootP application (supplied with the gateway's software package).
2. Add a client configuration for the gateway that you want to initialize.
3. Press the gateway's hardware Reset button to *physically* reset the gateway so that it uses BootP; the gateway changes its network parameters to the values provided by the BootP.

4.3.3 Assigning an IP Address Using the Voice Menu Guidance

Initial configuration of the gateway can be performed using a standard touch-tone telephone connected to one of the FXS analog ports. The voice menu can also be used to query and modify basic configuration parameters.



Note: Assigning an IP address using voice menu guidance is only possible when the gateway houses an FXS module (analog).

➤ **To assign an IP address using the voice menu guidance, take these 9 steps:**

1. Connect a telephone to one of the FXS ports.
2. Lift the handset and dial ***12345 (three stars followed by the digits 1, 2, 3, 4, 5).
3. Wait for the 'configuration menu' voice prompt to be played.
4. To change the IP address:
 - a. Press 1 followed by the pound key (#); The current IP address of the gateway is played.
 - b. Press # to change it.
 - c. Dial the new IP address. Use the star (*) key instead of dots ".", e.g., 192*168*0*4, and then press # to finish.
 - d. Review the new IP address, and then press 1 to save it.
5. To change the subnet mask:
 - a. Press 2 followed by the # key; The current subnet mask of the gateway is played.
 - b. Press # to change it.
 - c. Dial the new subnet mask (e.g., 255*255*0*0) and then press # to finish.
 - d. Review the new subnet mask, and then press 1 to save it.
6. To change the default Gateway IP address:
 - a. Press 3 followed by the # key; The current default Gateway address of the gateway is played.
 - b. Press # to change it.
 - c. Dial the new default Gateway address (e.g., 192*168*0*1), and then press # to finish.
 - d. Review the new default Gateway address, and then press 1 to save it.
7. Hang up the handset.
8. Access the gateway's Embedded Web Server with the new IP address you assigned (refer to 'Accessing the Embedded Web Server' on page 60).
9. Complete the gateway's configuration and save it to the non-volatile memory (refer to 'Saving Configuration' on page 278).

The following configuration parameters can be queried or modified via the voice menu:

Table 4-2: Configuration Parameters Available via the Voice Menu

| Item Number at Menu Prompt | Description |
|----------------------------|--|
| 1 | IP address |
| 2 | Subnet mask |
| 3 | Default Gateway IP address |
| 4 | Primary DNS server IP address |
| 7 | DHCP enable / disable |
| 11 | MGCP call agent IP address (N/A) |
| 12 | MGCP call agent port number (N/A) |
| 99 | Voice menu password (initially 12345). Note: The voice menu password can also be changed using the parameter VoiceMenuPassword (refer to 'Configuring the General Security Settings' on page 232). |

4.3.4 Assigning an IP Address Using the CLI

Assigning an IP address using the command-line interface (CLI) is performed in two stages:

1. Accessing the CLI (refer to 'Accessing the CLI' on page 53) using a standard Telnet application or serial communication software (e.g., HyperTerminal™) connected to the RS-232 port.
2. Assigning an IP address to the gateway (refer to 'Assigning an IP Address' on page 54).

4.3.4.1 Accessing the CLI

The procedure below describes how to access the CLI using either Telnet or RS-232 interface.

➤ **To access the CLI using the embedded Telnet server, take these 3 steps:**

1. Enable the embedded Telnet server, by performing the following:
 - a. Access the gateway's Embedded Web Server (refer to 'Accessing the Embedded Web Server' on page 60).
 - b. Open the 'Application Settings' screen (**Advanced Configuration** menu > **Network Settings** > **Application Settings** option), and therein set the parameter 'Embedded Telnet Server' to 'Enable (Unsecured)' or 'Enable Secured (SSL)'. For detailed information, refer to 'Configuring the Application Settings' on page 182.

- c. Save these settings to the flash memory and reset the gateway by performing the following:
 - a. Click the **Maintenance** button on the main menu bar; the 'Maintenance Actions' screen is displayed.
 - b. From the 'Burn to FLASH' drop-down list, select 'Yes', and then click the **Reset** button; the gateway shuts down and restarts.
2. Use a standard Telnet application to connect to the gateway's embedded Telnet server. Note that if the Telnet server is set to SSL mode, a special Telnet client is required on your PC to connect to the Telnet interface over a secured connection.
3. Login using the default username ('Admin') and password ('Admin').

The procedure below describes how to establish a serial communications link with the gateway (using serial communication software such as HyperTerminal™) through the RS-232 interface.

➤ **To access the CLI using the RS-232 port , take these 2 steps:**

1. Connect the gateway's RS-232 port to your PC (refer to Connecting the Mediant 1000 RS-232 Port to a PC on page 42 .
2. Use a serial communication software (e.g., HyperTerminal™) with the following communications port settings:
 - Baud Rate: 115,200 bps
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None

The CLI prompt appears.

4.3.4.2 Assigning an IP Address

Once you have accessed the CLI, follow the procedure below for assigning a new IP address.

➤ **To assign an IP address via the CLI, take these 4 steps:**

1. At the prompt, type **conf**, and then press <Enter>; the configuration folder is accessed.
2. To view the current network parameters, at the prompt, type **GCP IP**, and then press <Enter>; the current network settings are displayed.
3. Change the network settings by typing the following:
SCP IP [ip_address] [subnet_mask] [default_gateway]
For example,
SCP IP 10.13.77.7 255.255.0.0 10.13.0.1
The new settings take effect on-the-fly. Connectivity is active at the new IP address.
Note: This command requires you to enter all three network parameters (each separated by a space).
4. To save the configuration, at the prompt, type **SAR**, and then press <Enter>; the gateway restarts with the new network settings.

4.4 Configuring Basic Parameters

To configure the gateway's *basic* parameters, use the Embedded Web Server's 'Quick Setup' screen (shown in the figure below). For information on accessing the Embedded Web Server, refer to 'Accessing the Embedded Web Server' on page 60.

Figure 4-2: Quick Setup Screen

| Quick Setup | |
|----------------------------|-------------|
| IP Configuration | |
| IP Address | 10.4.4.113 |
| NAT IP Address | 0.0.0.0 |
| Subnet Mask | 255.255.0.0 |
| Default Gateway IP Address | 10.4.0.1 |
| SIP Parameters | |
| Gateway Name | |
| Working with Proxy | No |
| Proxy IP Address | 0.0.0.0 |
| Proxy Name | |
| Enable Registration | Disable |
| Tables | |
| Coders Table | --> |
| Tel to IP Routing Table | --> |
| Trunk Group Table | --> |

➤ **To configure basic SIP parameters, take these 11 steps:**

1. Access the 'Quick Setup' screen by clicking the **Quick Setup** menu.
2. If the gateway is connected to a router with NAT (Network Address Translation) enabled, perform the following (if it isn't, leave the 'NAT IP Address' field undefined):
 - Determine the 'public' IP address assigned to the router (by using, for example, router Web management). If the public IP address is static, enter this in the 'NAT IP Address' field.
 - Enable the DMZ (Demilitarized Zone) configuration on the router for the LAN port where the gateway is connected. This enables unknown packets to be routed to the DMZ port.
3. Under 'SIP Parameters', enter the gateway's domain name in the field 'Gateway Name'. If the field is not specified, the gateway's IP address is used instead (default).

4. When working with a Proxy server, set the 'Working with Proxy' field to 'Yes', and then enter the IP address of the primary Proxy server in the field 'Proxy IP address'. When no Proxy is used, the internal routing table is used to route the calls.
5. Enter the Proxy name in the field 'Proxy Name'. If Proxy name is used, it replaces the Proxy IP address in all SIP messages. This means that messages are still sent to the physical Proxy IP address, but the SIP URI contains the Proxy name instead.
6. Configure 'Enable Registration' to either one of the following:
 - 'Disable' = the gateway doesn't register to a Proxy server/Registrar (default).
 - 'Enable' = the gateway registers to a Proxy server/Registrar at power up and every 'Registration Time' seconds. For detailed information on the parameter 'Registration Time', refer to 'Proxy & Registration Parameters' on page [84](#).
7. To configure the Coders Table, click the arrow button next to 'Coders Table'. For information on how to configure the Coders Table, refer to 'Coders' on page [94](#).
8. To configure the Tel to IP Routing Table, click the arrow button next to 'Tel to IP Routing Table'. For information on how to configure the Tel to IP Routing Table, refer to 'Tel to IP Routing Table' on page [134](#).
9. To configure the E1/T1 B-channels, click the arrow button next to 'Trunk Group Table'. For information on how to configure the Trunk Group Table, refer to 'Configuring the Trunk Group Table' on page [150](#).
10. Click the **Reset** button, and then at the prompt, click **OK**; the gateway applies the changes and restarts.
11. After the gateway has reset, access the 'Trunk Settings' screen (Advanced Configuration > Trunk Settings), and select the gateway's E1/T1 protocol type and Framing method that best suits your system requirements. For information on how to configure the Trunk Settings, refer to 'Trunk Settings' on page [206](#).

You are now ready to start configuring the gateway. To prevent unauthorized access to the gateway, it's recommended that you change the default username and password used to access the Embedded Web Server. Refer to 'Configuring the Web User Accounts' on page [223](#) on how to change the username and password.



Tip: Once the gateway is configured correctly, back up your settings by saving a copy of the VoIP gateway configuration (*ini* file) to a directory on your PC. This saved file can be used to restore configuration settings at a later date. For information on backing up and restoring the gateway's configuration, refer to 'Restoring and Backing up Configuration' on page [280](#).

5 Web-based Management

The gateway's Embedded Web Server is used for remote configuration of the gateway including loading of configuration files, as well as for online monitoring of the gateway. In addition, you can also remotely reset the gateway. The Embedded Web Server can be accessed from a standard Web browser such as Microsoft™ Internet Explorer and Netscape™ Navigator.

5.1 Computer Requirements

To use the gateway's Embedded Web Server, the following is required:

- A computer capable of running your Web browser.
- A network connection to the gateway's Embedded Web Server.
- One of the following compatible Web browsers:
 - Microsoft™ Internet Explorer™ (version 6.0 or later)
 - Netscape™ Navigator™ (version 7.2 or later)
 - Mozilla Firefox® (version 1.5.0.10 or later)



Note: The Web browser must be javascript-enabled. If javascript is disabled, access to the Embedded Web Server is denied.

5.2 Protection and Security Mechanisms

Access to the gateway's Embedded Web Server is controlled by the following protection and security mechanisms:

- User accounts (refer to 'User Accounts' on page 58)
- Read-only mode (refer to 'Limiting the Embedded Web Server to Read-Only Mode' on page 59)
- Disabling access (refer to 'Disabling the Embedded Web Server' on page 59)
- Limiting access to a predefined list of IP addresses (refer to 'Configuring the Web and Telnet Access List' on page 225)
- Secured HTTP connection (HTTPS) (refer to the *SIP Series Reference Manual*)
- Managed access using a RADIUS server (refer to the *SIP Series Reference Manual*)

5.2.1 User Accounts

Up to five simultaneous users can be handled on gateway authentication via the Embedded Web Server. To prevent unauthorized access to the Embedded Web Server, two user accounts are available: primary and secondary. Each account is composed of three attributes: username, password, and access level. The username and password enable access to the Embedded Web Server itself; the access level determines the extent of the access (i.e., availability of screens and read / write privileges). Note that additional accounts can be defined using a RADIUS server (refer to the *SIP Series Reference Manual*).

The following table lists the available access levels and their privileges.

Table 5-1: Available Access Levels and their Privileges

| Access Level | Numeric Representation* | Privileges |
|--|-------------------------|---|
| Security Administrator | 200 | Read / write privileges for all screens |
| Administrator | 100 | Read-only privilege for security-related screens and read / write privileges for the others |
| User Monitor | 50 | No access to security-related and file-loading screens and read-only access to the others |
| No Access | 0 | No access to any screen |
| * The numeric representation of the access level is used only to define accounts in a RADIUS server (the access level ranges from 1 to 255). | | |

Each Web screen features two (hard-coded) minimum access levels, read and write. The read access level determines whether the screen can be viewed. The write access level determines whether the information in the screen can be modified. When a user tries to access a specific Web screen, the user's access level is compared with the access levels of the screen:

- If the access level of the user is less than the screen's read access level, the screen cannot be viewed.
- If the access level of the user is equal to or greater than the screen's read access level but less than the write access level, the screen is read only.
- If the access level of the user is equal to or greater than the screen's write access level, the screen can be modified.

The default attributes for the two accounts are shown in the following table:

Table 5-2: Default Attributes for the Accounts

| Account / Attribute | Username (Case-Sensitive) | Password (Case-Sensitive) | Access Level |
|--|---------------------------|---------------------------|-------------------------|
| Primary Account | Admin | Admin | Security Administrator* |
| Secondary Account | User | User | User Monitor |
| * The access level of the primary account cannot be changed; all other account-attributes can be modified. | | | |

The first time a Web browser request is made, users are requested to provide their account's username and password to obtain access. If the Embedded Web Server is left idle for more than five minutes, the session expires and the user is required to re-enter username and password.



Tip: To access the Embedded Web Server with a different account, click the **Log Off** button and re-access with a new username and password.

For details on changing the account attributes, refer to 'Configuring the Web User Accounts' on page 223. Note that the password and username can be a maximum of 19 case-sensitive characters.

To reset the username and password of both accounts to their defaults, set the *ini* file parameter `ResetWebPassword` to 1.

5.2.2 Limiting the Embedded Web Server to Read-Only Mode

Users can limit access to the Embedded Web Server to read-only mode by changing the *ini* file parameter `DisableWebConfig` to 1. In this mode, all Web screens, regardless of the access level used, are read-only and cannot be modified. In addition, the following screens cannot be accessed: 'Quick Setup', 'Web User Accounts', 'Maintenance Actions' and all file-loading screens.



Notes:

- Read-only policy can also be applied to selected users by setting the access level of the secondary account to 'User Monitor' (`DisableWebConfig = 0`) and distributing the primary and secondary accounts to users according to the organization's security policy.
- When `DisableWebConfig` is set to 1, read-only privileges are applied to all accounts regardless of their access level.

5.2.3 Disabling the Embedded Web Server

Access to the Embedded Web Server can be disabled by setting the *ini* file parameter `DisableWebTask` to 1. By default, the access is enabled.

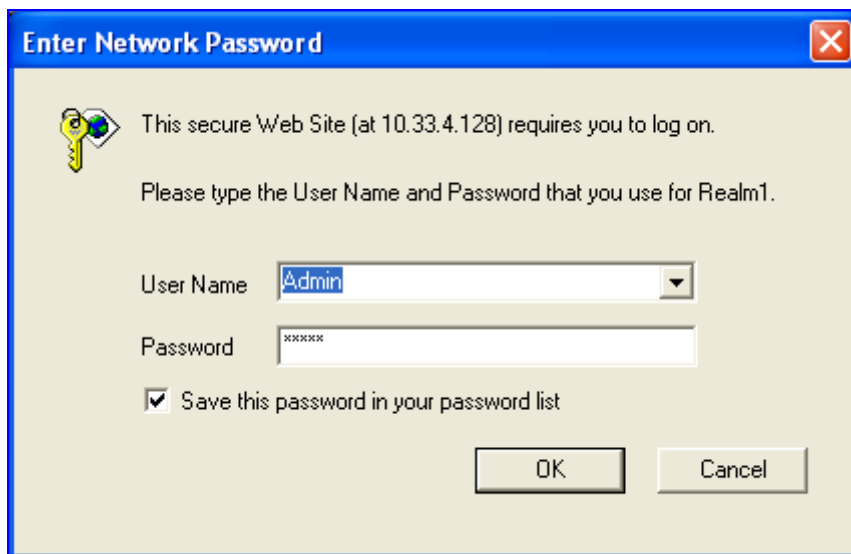
5.3 Accessing the Embedded Web Server

You can access the gateway's Embedded Web Server by following the procedure below.

➤ **To access the Embedded Web Server, take these 4 steps:**

1. Open a standard Web-browsing application (for a list of supported Web browsers, refer to 'Computer Requirements' on page 57).
2. In the Web browser's Uniform Resource Locator (URL) field, specify the gateway's IP address (e.g., <http://10.1.10.10>); the Embedded Web Server's 'Enter Network Password' screen appears, as shown in the figure below.

Figure 5-1: Enter Network Password Screen



3. In the 'User Name' and 'Password' fields, enter the username (default: 'Admin') and password (default: 'Admin'). Note that the username and password are case-sensitive.
4. Click the **OK** button; the Embedded Web Server is accessed, displaying the Home page (for a detailed description of the Home page, refer to Using the Home Page on page 282).



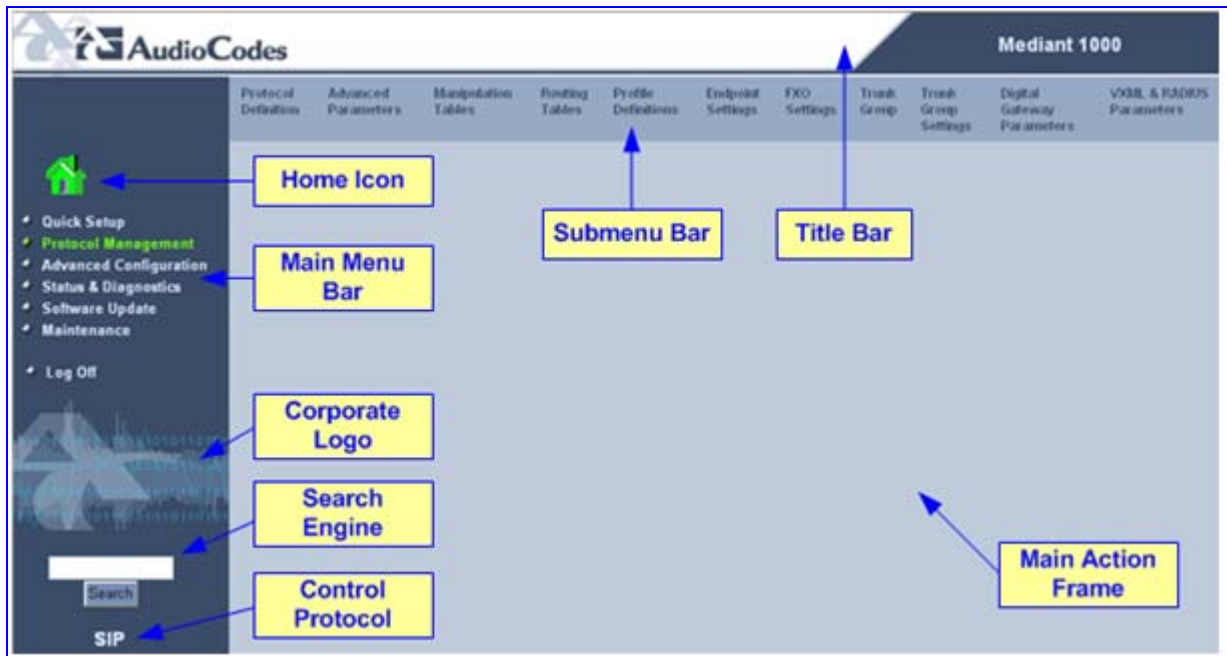
Note: If access to the gateway's Embedded Web Server is denied ("Unauthorized") due to Microsoft Internet Explorer security settings, perform the following troubleshooting procedures:

1. Delete all cookies in the Temporary Internet Files folder. If this does not resolve the problem, the security settings may need to be altered (continue with Step 2).
2. In Internet Explorer, navigate to **Tools** menu > **Internet Options** > **Security** tab > **Custom Level**, and then scroll down to the Logon options and select **Prompt for username and password**. Select the **Advanced** tab, and then scroll down until the HTTP 1.1 Settings are displayed and verify that **Use HTTP 1.1** is selected.
3. Quit and start the Web browser again.

5.4 Getting Acquainted with the Web Interface

The figure below displays the general layout of the interface of the Embedded Web Server.

Figure 5-2: Areas of the Web-based User Interface



The Embedded Web Server features the following components:

- **Title bar:** contains three configurable elements: corporate logo, a background image, and the product's name. For information on how to modify these elements, refer to 'Customizing the Web Interface' on page 65.
- **Main menu bar:** contains the main menus (refer to 'Main Menu Bar' on page 62).
- **Submenu bar:** contains submenus pertaining to the selected main menu (from the Main menu bar). Each submenu provides a list of drop-down options that access configuration screens.
- **Main action frame:** main area of the Embedded Web Server in which configuration screens are displayed.
- **Home icon:** opens the Home page screen used mainly for monitoring the gateway (refer to Using the Home Page on page 282).
- **Corporate logo:** AudioCodes' corporate logo. For information on how to remove this logo, refer to 'Customizing the Web Interface' on page 65.
- **Search engine:** used for searching *ini* file parameters that have corresponding Embedded Web Server parameters (refer to 'Searching for Configuration Parameters' on page 63).
- **Control Protocol:** the gateway's control protocol (i.e., SIP).

5.4.1 Main Menu Bar

The main menu bar of the Embedded Web Server provides the following menus:

- **Quick Setup:** Accesses the 'Quick Setup' screen for quickly configuring the gateway's basic settings. For a full list of configurable parameters, directly access the Protocol Management and Advanced Configuration menus. An example of the Quick Setup configuration is described in 'Configuring the Basic Parameters' on page 55.
- **Protocol Management:** used to configure the gateway's control protocol parameters and tables (refer to 'Protocol Management' on page 71).
- **Advanced Configuration:** used to configure the gateway's advanced configuration parameters.
- **Status & Diagnostics:** use to view Syslog messages, hardware / software product information, and to assess the gateway's statistics and IP connectivity information (refer to 'Status & Diagnostics' on page 251).
- **Software Update:** used to load new software or configuration files to the gateway (refer to 'Software Update' on page 262).
- **Maintenance:** used to remotely lock/unlock the gateway (refer to 'Locking and Unlocking the Gateway' on page 276), save configuration changes to the non-volatile flash memory (refer to 'Saving Configuration' on page 278), and reset the gateway (refer to 'Resetting the Gateway' on page 279).

5.4.2 Saving Changes

To apply changes to the gateway's volatile memory (RAM), click the **Submit** button that appears in the screen in which you are working. Modifications to parameters with on-the-fly capabilities are immediately applied to the gateway; other parameters are updated only after a gateway reset.

Parameters saved to the volatile memory (i.e., not burned to flash memory), revert to their previous settings after a hardware reset (or if the gateway is powered down). However, when performing a software reset (i.e., using the Embedded Web Server or SNMP), you can also choose to save the parameter settings to the non-volatile memory (i.e., flash). To save the changes to flash, refer to 'Saving Configuration' on page 278.



Note: Parameters preceded by an exclamation mark (!) are not changeable on-the-fly and require that the device be reset.

5.4.3 Entering Phone Numbers in Various Tables

Phone numbers or prefixes entered into various tables on the gateway such as the Tel to IP routing table, must be entered without any formatting characters. For example, if you wish to enter the phone number 555-1212, it must be entered as 5551212 without the hyphen (-). If the hyphen is entered, the entry is not valid. The hyphen character is used in number entry only, as part of a range definition. For example, the entry [20-29] means 'all numbers in the range 20 to 29'.

5.4.4 Searching for Configuration Parameters

The Embedded Web Server provides a search engine that allows you to search any *ini* file parameter that is configurable by the Web server. The **Search** button, located near the bottom of the Main menu bar is used to perform parameter searches.

You can search for a specific parameter (e.g., "EnableIPSec") or a sub-string of that parameter (e.g., "sec"). If you search for a sub-string, the Embedded Web Server lists all parameters that contain the searched sub-string in their parameter names.

➤ **To search for ini file parameters configurable in the Embedded Web Server, take these 3 steps:**

1. In the Search Engine field, enter the parameter name or sub-string of the parameter name.
2. Click **Search**. The Searched Result screen appears, listing all searched parameter results, as shown in the example below:

Figure 5-3: Searched Result Screen



Each searched result displays the following:

- Parameter name (hyperlinked to its location in the Embedded Web Server)
- Brief description of the parameter
- Hyperlink in green displaying the URL path to its location in the Embedded Web Server location

3. In the searched result list, click the required parameter to open the screen in which the parameter appears; the searched parameter is highlighted in green in the screen for easy identification, as shown in the figure below.

Figure 5-4: Searched Parameter Highlighted in Screen

| IP Settings | |
|-------------------------|--|
| IP Networking Mode | Single IP Network <input type="button" value="v"/> |
| IP Address | 10.33.4.128 |
| Subnet Mask | 255.255.0.0 |
| Default Gateway Address | 10.33.0.1 |
| DNS Settings | |
| DNS Primary Server IP | <input type="text"/> |
| DNS Secondary Server IP | <input type="text"/> |
| DHCP Settings | |
| Enable DHCP | Disable <input type="button" value="v"/> |
| NAT Settings | |
| NAT IP Address | 0.0.0.0 |
| Differential Services | |
| Network QoS | 48 |
| Media Premium QoS | 46 |
| Control Premium QoS | 40 |
| Gold QoS | 26 |
| Bronze QoS | 10 |



Note: If the searched parameter is not located, the "No Matches Found For This String" message is displayed.



Tip: When moving your cursor over a parameter name (or table) for more than a second, a short description of the parameter is briefly displayed.

5.4.5 Customizing the Web Interface

You can customize the gateway's Embedded Web Server interface to suit your specific corporate logo and product naming conventions. The following Web interface elements can be customized:

- Main corporate logo displayed on the title bar (refer to 'Replacing the Main Corporate Logo' on page 65)
- Background image displayed on the title bar (refer to 'Replacing the Background Image File' on page 68)
- Product's name displayed on the title bar (refer to 'Customizing the Product Name' on page 69)
- Login welcome message (refer to 'Creating a Login Welcome Message' on page 70)

The figure below displays an example of the default title bar (i.e., of AudioCodes) and below it, a customized one:

Figure 5-5: Customized Web Interface Title Bar

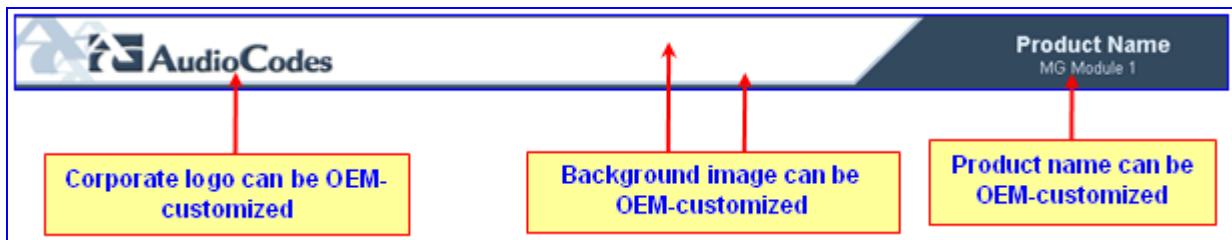


Figure 5-6: Customized Web Interface Title Bar



5.4.5.1 Replacing the Main Corporate Logo

The main corporate logo can be replaced either with a different logo image file (refer to 'Replacing the Main Corporate Logo with an Image File' on page 66) or with a text string (refer to 'Replacing the Main Corporate Logo with a Text String' on page 67).



Notes:

- When the main corporation logo is replaced, AudioCodes' logo on the left bar (refer to 'Getting Acquainted with the Web Interface' on page 61) and in the Software Upgrade Wizard (refer to 'Software Upgrade Wizard' on page 262) disappear.
- The Web browser's title bar is automatically updated with the string assigned to the WebLogoText parameter when AudioCodes' default logo is not used.

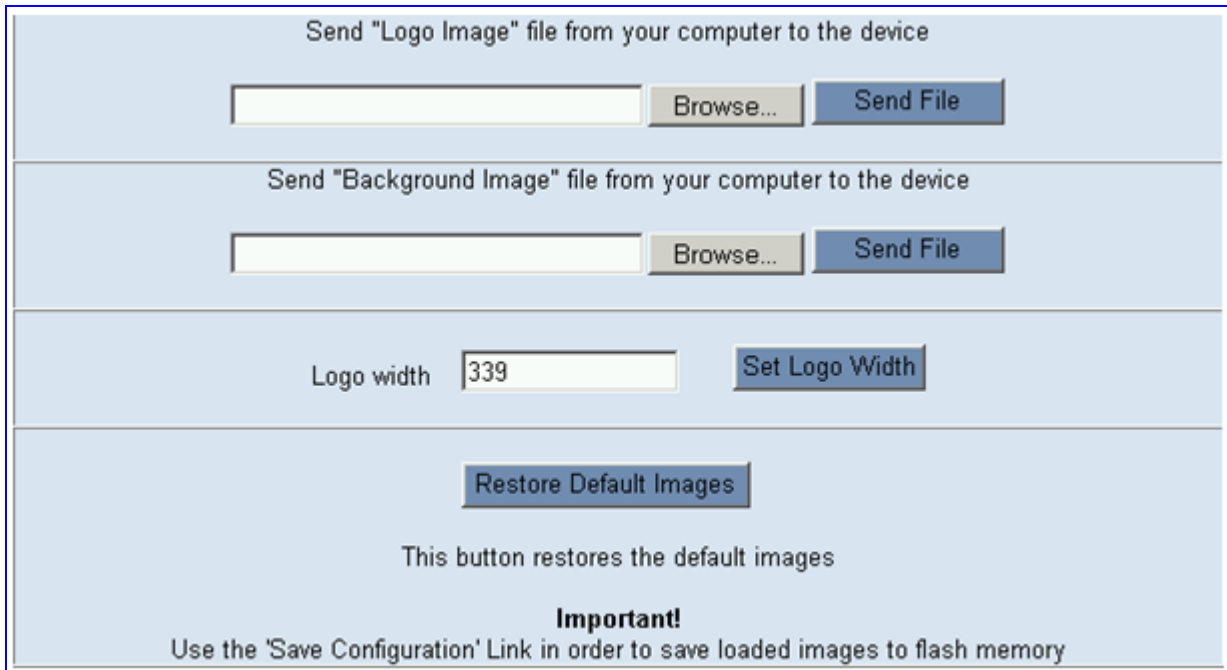
5.4.5.1.1 Replacing the Main Corporate Logo with an Image File

You can replace the logo in the Web interface's title bar using either the Embedded Web Server or the *ini* file.

➤ **To replace the default logo with your own corporate image via the Embedded Web Server, take these 7 steps:**

1. Access the gateway's Embedded Web Server (refer to 'Accessing the Embedded Web Server' on page 60).
2. In the URL field, append the case-sensitive suffix 'AdminPage' to the IP address (e.g., <http://10.1.229.17/AdminPage>).
3. Click **Image Load to Device**; the Image Download screen is displayed, as shown in the figure below.

Figure 5-7: Image Download Screen



The screenshot shows a web interface for uploading images to a device. It has a light blue background and is divided into several sections. The top section is titled "Send 'Logo Image' file from your computer to the device" and contains a text input field, a "Browse..." button, and a "Send File" button. The second section is titled "Send 'Background Image' file from your computer to the device" and also contains a text input field, a "Browse..." button, and a "Send File" button. The third section is titled "Logo width" and contains a text input field with the value "339" and a "Set Logo Width" button. The fourth section contains a "Restore Default Images" button. Below this button, there is a line of text: "This button restores the default images". At the bottom of the screen, there is a bold heading "Important!" followed by the text "Use the 'Save Configuration' Link in order to save loaded images to flash memory".

4. Click the **Browse** button in the 'Send Logo Image File from your computer to the Device' box. Navigate to the folder that contains the logo image file you want to load.
5. Click the **Send File** button; the file is sent to the device. When loading is complete, the screen is automatically refreshed and the new logo image is displayed.
6. If you want to modify the width of the logo (the default width is 339 pixels), in the 'Logo Width' field, enter the new width (in pixels) and then click the **Set Logo Width** button.
7. To save the image to flash memory, refer to 'Saving Configuration' on page 278.

The new logo appears on all Embedded Web Server interface pages.



Note: Use a gif, jpg or jpeg file for the logo image. It is important that the image file has a fixed height of 59 pixels (the width can be configured up to a maximum of 339 pixels). The size of the image files (logo and background) is limited each to 64 Kbytes.



Tip: If you encounter any problem during the loading of the files or you want to restore the default images, click the **Restore Default Images** button.

➤ **To replace the default logo with your own corporate image via the *ini* file, take these 3 steps:**

1. Place your corporate logo image file in the same folder as where the device's *ini* file is located (i.e., the same location defined in the BootP/TFTP configuration utility). For detailed information on the BootP/TFTP, refer to the *SIP Series Reference Manual*.
2. Add or modify the *ini* file parameters described in the table below (as described in 'Modifying an ini File' on page 293).
3. Load the *ini* file using only BootP / TFTP (i.e., not through the Embedded Web Server).

Table 5-3: Customizable Logo ini File Parameters

| Parameter | Description |
|---------------------|--|
| LogoFileName | The name of the image file containing your corporate logo. Use a gif, jpg or jpeg image file. The default is AudioCodes' logo file. Note: The length of the name of the image file is limited to 47 characters. |
| LogoWidth | Width (in pixels) of the logo image. The default value is 339 (which is the width of AudioCodes' displayed logo). Note: The optimal setting depends on the resolution settings. |

5.4.5.1.2 Replacing the Main Corporate Logo with a Text String

The main corporate logo can be replaced with a text string. To replace AudioCodes' default logo with a text string using the *ini* file, add or modify the two *ini* file parameters listed in the table below (according to the procedure described in 'Modifying an ini File' on page 293).

Table 5-4: Web Appearance Customizable ini File Parameters

| Parameter | Description |
|--------------------|---|
| UseWebLogo | <ul style="list-style-type: none"> ▪ [0] = Logo image is used (default). ▪ [1] = Text string is used instead of a logo image. |
| WebLogoText | Text string that replaces the logo image. The string can be up to 15 characters. |

5.4.5.2 Replacing the Background Image File

The background image file is duplicated across the width of the screen. The number of times the image is duplicated depends on the width of the background image and screen resolution. When choosing your background image, keep this in mind. The background image file can be replaced using either the Embedded Web Server or the *ini* file.



Note: Use a gif, jpg or jpeg file for the background image. It is important that the image file has a fixed height of 59 pixels. The size of the image files (logo and background) is limited each to 64 Kbytes.

➤ **To replace the background image using the Embedded Web Server, take these 6 steps:**

1. Access the gateway's Embedded Web Server (refer to 'Accessing the Embedded Web Server' on page 60).
2. In the Web browser's URL field, append the case-sensitive suffix 'AdminPage' to the IP address (e.g., <http://10.1.229.17/AdminPage>).
3. Click the **Image Load to Device**; the 'Image Download' screen is displayed (shown in 'Replacing the Main Corporate Logo with an Image File' on page 66).
4. Click the **Browse** button in the 'Send Background Image File from your computer to box', and then navigate to the folder that contains the background image file you want to load.
5. Click the **Send File** button; the file is sent to the device. When loading is complete, the screen is automatically refreshed and the new background image is displayed.
6. To save the image to flash memory, refer to 'Saving Configuration' on page 278.

The new background appears on all Embedded Web Server interface pages.



Tips:

- If you encounter any problem during the loading of the files or you want to restore the default images, click the **Restore Default Images** button.
- When replacing both the background image and the logo image, first load the logo image followed by the background image.

- **To replace the background image via the *ini* file, take these 3 steps:**
1. Place your background image file in the same folder as where the device's *ini* file is located (i.e., the same location defined in the BootP/TFTP configuration utility). For detailed information on the BootP/TFTP, refer to the *SIP Series Reference Manual*).
 2. Add or modify the *ini* file parameters listed in the table below (according to the procedure described in 'Modifying an ini File' on page 293).
 3. Load the *ini* file using only BootP / TFTP (i.e., not through the Embedded Web Server).

Table 5-5: Customizable Logo ini File Parameters

| Parameter | Description |
|-------------------------|--|
| BkgImageFileName | The name (and path) of the file containing the new background. Use a gif, jpg or jpeg image file. The default is AudioCodes background file. Note: The length of the name of the image file is limited to 47 characters. |

5.4.5.3 Customizing the Product Name

To replace AudioCodes' default product name with a text string, add or modify the two *ini* file parameters listed in the table below (according to the procedure described in 'Modifying an ini File' on page 293).

Table 5-6: Web Appearance Customizable ini File Parameters

| Parameter | Description |
|------------------------|---|
| UseProductName | <ul style="list-style-type: none"> ▪ [0] = Don't change the product name (default). ▪ [1] = Enable product name change. |
| UserProductName | Text string that replaces the product name. The default is 'Mediant 1000'. The string can be up to 29 characters. |

5.4.5.4 Creating a Login Welcome Message

You can create a Welcome message box (alert message) that appears (see figure below for an example) after each successful login to the gateway's Embedded Web Server. The *ini* file parameter table WelcomeMessage allows you to create the Welcome message. Up to 20 lines of character strings can be defined for the message. If this parameter is not configured, no Welcome message box is displayed after login.

Figure 5-8: User-Defined Web Welcome Message after Login

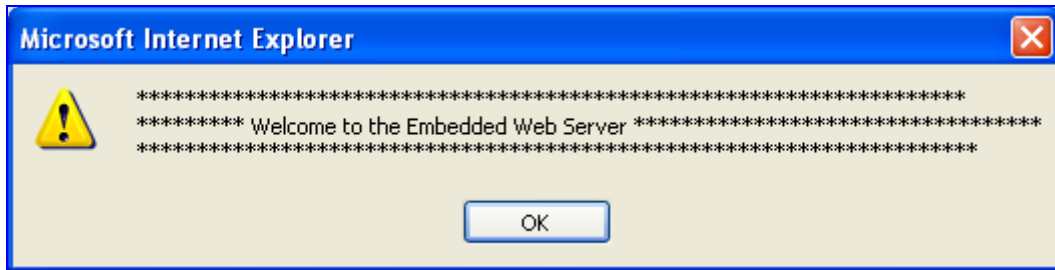


Table 5-7: User-Defined Welcome Message ini File Parameter

| Parameter | Description |
|-----------------------|--|
| WelcomeMessage | <p>Configures the Welcome message that appears after a Embedded Web Server login.</p> <p>The format of this <i>ini</i> file parameter table is:</p> <pre>[WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text WelcomeMessage 1 = "..."; WelcomeMessage 2 = "..."; WelcomeMessage 3 = "..."; [WelcomeMessage]</pre> <p>For Example:</p> <pre>[WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text WelcomeMessage 1 = "*****"; WelcomeMessage 2 = "***** This is a Welcome message *****"; WelcomeMessage 3 = "*****"; [WelcomeMessage]</pre> <p>Note: Each index represents a line of text in the Welcome message box. Up to 20 indexes can be defined.</p> |

5.5 Protocol Management

The **Protocol Management** menu is used to configure the gateway's SIP parameters and tables.



Note: Throughout this section, parameters enclosed in square brackets ([...]) depict the *ini* file parameters that correspond to the Embedded Web Server parameters. For configuration using the *ini* file, refer to 'ini File Configuration' on page 293.

5.5.1 Protocol Definition Parameters

The **Protocol Definition** submenu is used to configure the following SIP protocol parameters:

- General (refer to 'General Parameters' on page 72)
- Proxy & Registration (refer to 'Proxy & Registration Parameters' on page 84)
- Coders (refer to 'Coders' on page 94)
- DTMF & Dialing (refer to 'DTMF & Dialing Parameters' on page 98)

5.5.1.1 General Parameters

The **General Parameters** option is used to configure general SIP parameters.

➤ **To configure the general SIP protocol parameters, take these 4 steps:**

1. Open the 'General Parameters' screen (**Protocol Management** menu > **Protocol Definition** submenu > **General Parameters** option).

Figure 5-9: General Parameters Screen (Protocol Definition Submenu)

| General | |
|--|----------------------------|
| PRACK Mode | Disable |
| Channel Select Mode | Cyclic Ascending |
| Enable Early Media | Disable |
| 183 Message Behavior | Progress |
| Session-Expires Time | 0 |
| Minimum Session-Expires | 90 |
| Session Expires Method | Re-Invite |
| Asserted Identity Mode | Disabled |
| Fax Signaling Method | No Fax |
| ! Detect Fax on Answer Tone | Initiate T.38 on Preamble |
| SIP Transport Type | UDP |
| SIP UDP Local Port | 5060 |
| SIP TCP Local Port | 5060 |
| SIP TLS Local Port | 5061 |
| Enable SIPS | Disable |
| Enable TCP Connection Reuse | Enable |
| ! TCP Timeout | 0 |
| SIP Destination Port | 5060 |
| Use "user=phone" in SIP URL | Yes |
| Use "user=phone" in From Header | No |
| Use Tel URI for Asserted Identity | Disable |
| Tel to IP No Answer Timeout | 180 |
| Enable Remote Party ID | Enable |
| Add Number Plan and Type to Remote Party ID Header | Yes |
| Enable History-Info Header | Disable |
| Use Source Number as Display Name | No |
| Use Display Name as Source Number | No |
| Play Ringback Tone to IP | Don't Play |
| Play Ringback Tone to Tel | Play According to Early Me |
| Use Tgrp information | Disable |
| Enable GRUU | Disable |
| User-Agent Information | |
| SDP Session Owner | AudiocodesGW |
| Play Busy Tone to Tel | Don't Play |
| Subject | |
| Multiple Packetization Time Format | None |
| Enable Reason Header | Enable |
| Enable Semi-Attended Transfer | Disable |
| 3xx Behavior | Forward |
| Enable P-Charging Vector | Disable |
| Enable VoiceMail URI | Disable |
| Retransmission Parameters | |
| SIP T1 Retransmission Timer [msec] | 500 |
| SIP T2 Retransmission Timer [msec] | 4000 |
| SIP Maximum RTX | 7 |

2. Configure the parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|---|--|
| PRACK Mode [PRACKMode] | <p>PRACK mechanism mode for 1xx reliable responses. Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Supported (default) ▪ [2] Required <p>Notes:</p> <ul style="list-style-type: none"> ▪ The Supported and Required headers contain the '100rel' parameter. ▪ The gateway sends PRACK message if 180/183 response is received with '100rel' in the Supported or the Required headers. |
| Channel Select Mode [ChannelSelectMode] | <p>Port allocation algorithm for IP-to-Tel calls. You can select one of the following methods:</p> <ul style="list-style-type: none"> ▪ [0] By Dest Phone Number = (default) Select the gateway port according to the called number (called number is defined in the 'Endpoint Phone Number' table). ▪ [1] Cyclic Ascending = Select the next available channel in an ascending cycle order. Always select the next higher channel number in the trunk group. When the gateway reaches the highest channel number in the trunkgroup, it selects the lowest channel number in the trunkgroup and then starts ascending again. ▪ [2] Ascending = Select the lowest available channel. Always start at the lowest channel number in the trunk group and if that channel is not available, select the next higher channel. ▪ [3] Cyclic Descending = Select the next available channel in descending cycle order. Always select the next lower channel number in the trunk group. When the gateway reaches the lowest channel number in the hunt group, it selects the highest channel number in the trunk group and then starts descending again. ▪ [4] Descending = Select the highest available channel. Always start at the highest channel number in the trunk group and if that channel is not available, select the next lower channel. ▪ [5] Dest Number + Cyclic Ascending = First select the gateway port according to the called number. If the called number isn't found, then select the next available channel in ascending cyclic order. Note that if the called number is found, but the port associated with this number is busy, the call is released. ▪ [6] By Source Phone Number = Select the gateway port according to the calling number. ▪ [7] Trunk Cyclic Ascending = Digital: Select the gateway port from the first channel of the next trunk (next to the trunk from which the previous channel was allocated. Analog: N/A. <p>Note: The internal numbers of the gateway's B-channels are defined by the TrunkGroup parameter.</p> |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|---|---|
| Enable Early Media [EnableEarlyMedia] | <p>If enabled, the gateway sends 183 Session Progress response with SDP (instead of 180 Ringing), allowing the media stream to be set up prior to the answering of the call.</p> <ul style="list-style-type: none"> [0] Disable = Early Media is disabled (default). [1] Enable = Enables Early Media. <p>For Analog interface: Note that to send 183 response you must also set the parameter ProgressIndicator2IP to 1. If it is equal to 0, 180 Ringing response is sent.</p> <p>For Digital interface: Sending a 183 response depends on the Progress Indicator. It is sent only if PI = 1 or PI = 8 is received in Proceeding or Alert PRI messages. For CAS gateways, see the ProgressIndicator2IP parameter.</p> |
| 183 Message Behavior [SIP183Behavior] | <p>Defines the ISDN message that is sent when 183 Session Progress message is received for IP-to-Tel calls.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> [0] Progress = Progress message (default). [1] Alert = Alert message. <p>When set to 1, the gateway sends an Alert message (after the receipt of a 183 response) instead of an ISDN Progress message.</p> |
| Session-Expires Time [SIPSessionExpires] | <p>Determines the timeout (in seconds) for keeping a Re-INVITE message alive within a SIP session. The SIP session is refreshed each time this timer expires. The SIP method used for session-timer updates is determined according to the parameter SessionExpiresMethod. The valid range is 1 to 86400 sec. The default is 0 (i.e., not activated).</p> |
| Minimum Session-Expires [MINSE] | <p>Defines the time (in seconds) that is used in the Min-SE header. This header defines the minimum time that the user agent supports for session refresh.</p> <p>The valid range is 10 to 100000. The default value is 90.</p> |
| Session Expires Method [SessionExpiresMethod] | <p>Defines the SIP method used for session-timer updates.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> [0] Re-Invite = Use Re-INVITE messages for session-timer updates (default). [1] Update = Use UPDATE messages. <p>Notes:</p> <ul style="list-style-type: none"> The gateway can receive session-timer refreshes using both methods. The UPDATE message used for session-timer purposes is excluded from the SDP body. |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|---|---|
| Asserted Identity Mode [AssertedIdMode] | <ul style="list-style-type: none"> ▪ [0] Disabled = None (default) ▪ [1] Adding PAsserted Identity ▪ [2] Adding PPreferred Identity <p>The Asserted ID mode defines the header that is used in the generated INVITE request. The header also depends on the calling Privacy: allowed or restricted.</p> <p>The P-asserted (or P-preferred) headers are used to present the originating party's Caller ID. The Caller ID is composed of a Calling Number and (optionally) a Calling Name.</p> <p>P-asserted (or P-preferred) headers are used together with the Privacy header. If Caller ID is restricted, the 'Privacy: id' is included. Otherwise for allowed Caller ID, the 'Privacy: none' is used. If Caller ID is restricted (received from Tel or configured in the gateway), the From header is set to <anonymous@anonymous.invalid>.</p> |
| Fax Signaling Method [IsFaxUsed] | <p>Determines the SIP signaling method used to establish and convey a fax session after a fax is detected.</p> <ul style="list-style-type: none"> ▪ [0] No Fax = No fax negotiation using SIP signaling. Fax transport method is according to the parameter FaxTransportMode (default). ▪ [1] T.38 Relay = Initiates T.38 fax relay. ▪ [2] G.711 Transport = Initiates fax / modem using the coder G.711 A-law/μ-law with adaptations (refer to Note below). ▪ [3] Fax Fallback = Initiates T.38 fax relay. If the T.38 negotiation fails, the gateway re-initiates a fax session using the coder G.711 A-law/μ-law with adaptations (refer to Note below). <p>Notes:</p> <ul style="list-style-type: none"> ▪ Fax adaptations (for options 2 and 3): Echo Canceller = On Silence Compression = Off Echo Canceller Non-Linear Processor Mode = Off Dynamic Jitter Buffer Minimum Delay = 40 Dynamic Jitter Buffer Optimization Factor = 13 ▪ If the gateway initiates a fax session using G.711 (option 2 and possibly 3), a 'gpmd' attribute is added to the SDP in the following format: For A-law: 'a=gpmd:0 vbd=yes;ecan=on'. For μ-law: 'a=gpmd:8 vbd=yes;ecan=on'. ▪ When IsFaxUsed is set to 1, 2, or 3 the parameter FaxTransportMode is ignored. ▪ When the value of IsFaxUsed is other than 1, T.38 might still be used without the control protocol's involvement. To completely disable T.38, set FaxTransportMode to a value other than 1. ▪ For detailed information on fax transport methods, refer to 'Fax/Modem Transport Modes' on page 381. |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|--|---|
| Detect Fax on Answer Tone [DetFaxOnAnswerTone] | <ul style="list-style-type: none"> [0] Initiate T.38 on Preamble = Terminating fax gateway initiates T.38 session on receiving HDLC preamble signal from fax (default) [1] Initiate T.38 on CED = Terminating fax gateway initiates T.38 session on receiving CED answer tone from fax. <p>Note: This parameters is applicable only if IsFaxUsed = 1.</p> |
| SIP Transport Type [SIPTransportType] | Determines the <i>default</i> transport layer used for outgoing SIP calls initiated by the gateway. Valid options include: <ul style="list-style-type: none"> [0] UDP (default) [1] TCP [2] TLS (SIPS) <p>Note: It's recommended to use TLS to communicate with a SIP Proxy and not for direct gateway-gateway communication.</p> |
| SIP UDP Local Port [LocalSIPPort] | Local UDP port used to receive SIP messages. The valid range is 1 to 65534. The default value is 5060. |
| SIP TCP Local Port [TCPLocalSIPPort] | Local TCP port used to receive SIP messages. The default value is 5060. |
| SIP TLS Local Port [TLSTLocalSIPPort] | Local TLS port used to receive SIP messages. The default value is 5061. <p>Note: The value of TLSTLocalSIPPort must be different to the value of TCPLocalSIPPort.</p> |
| Enable SIPS [EnableSIPS] | Enables secured SIP (SIPS) connections over multiple hops. <ul style="list-style-type: none"> [0] Disable (default). [1] Enable. <p>When SIPTransportType = 2 (TLS) and EnableSIPS is disabled, TLS is used for the next network hop only. When SIPTransportType = 2 (TLS) or 1 (TCP) and EnableSIPS is enabled, TLS is used through the entire connection (over multiple hops).</p> <p>Note: If SIPS is enabled and SIPTransportType = UDP, the connection fails.</p> |
| Enable TCP Connection Reuse [EnableTCPConnectionReuse] | Enables the reuse of the same TCP connection for all calls to the same destination. Valid options include: <ul style="list-style-type: none"> [0] Disable = Use a separate TCP connection for each call (default) [1] Enable = Use the same TCP connection for all calls |
| TCP Timeout [SIPTCPTimeout] | Defines the Timer B and Timer F (as defined in RFC 3261) when the SIP Transport Type is TCP. The valid range is 0 to 40 sec. The default value is SIPT1Rtx * 64 msec. |
| SIP Destination Port [SIPDestinationPort] | SIP destination port for sending initial SIP requests. The valid range is 1 to 65534. The default port is 5060. <p>Note: SIP responses are sent to the port specified in the Via header.</p> |
| Use "user=phone" in SIP URL [IsUserPhone] | <ul style="list-style-type: none"> [0] No = 'user=phone' string isn't used in SIP URI. [1] Yes = 'user=phone' string is part of the SIP URI (default). |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|---|--|
| Use "user=phone" in From Header [IsUserPhoneInFrom] | <ul style="list-style-type: none"> [0] No = Doesn't use ';user=phone' string in From header (default). [1] Yes = ';user=phone' string is part of the From header. |
| Use Tel URI for Asserted Identity [UseTelURIForAssertedID] | <p>Determines the format of the URI in the P-Asserted and P-Preferred headers.</p> <ul style="list-style-type: none"> [0] Disable = 'sip:' (default). [1] Enable = 'tel:'. |
| Tel to IP No Answer Timeout [IPAlertTimeout] | <p>Defines the time (in seconds) the gateway waits for a 200 OK response from the called party (IP side) after sending an INVITE message. If the timer expires, the call is released.</p> <p>The valid range is 0 to 3600. The default value is 180.</p> |
| Enable Remote Party ID [EnableRPIheader] | <p>Enable Remote-Party-ID (RPI) headers for calling and called numbers for Tel→IP calls.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> [0] Disable (default). [1] Enable = RPI headers are generated in SIP INVITE messages for both called and calling numbers. |
| Add Number Plan and Type to Remote Party ID Header [AddTON2RPI] | <ul style="list-style-type: none"> [0] No = TON/PLAN parameters aren't included in the RPID header. [1] Yes = TON/PLAN parameters are included in the RPID header (default). <p>If RPID header is enabled (EnableRPIHeader = 1) and AddTON2RPI = 1, it's possible to configure the calling and called number type and number plan using the Number Manipulation tables for Tel→IP calls.</p> |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description | | | | | | | | | | |
|--|---|-----------------|-------------------------|-------------------------|------------------------------|-----------------------|-------------------------------|-------------------------------|-----------------|-------------------------|-----------------------|
| Enable History-Info Header [EnableHistoryInfo] | <p>Enables usage of the History-Info header. Valid options include:</p> <ul style="list-style-type: none"> [0] Disable = Disable (default) [1] Enable = Enable <p>UAC Behavior:</p> <ul style="list-style-type: none"> Initial request: The History-Info header is equal to the Request URI. If a PSTN Redirect number is received, it is added as an additional History-Info header with an appropriate reason. Upon receiving the final failure response, the gateway copies the History-Info as is, adds the reason of the failure response to the last entry, and concatenates a new destination to it (if an additional request is sent). The order of the reasons is as follows: <ul style="list-style-type: none"> - Q.850 Reason - SIP Reason - SIP Response code Upon receiving the final (success or failure) response, the gateway searches for a Redirect reason in the History-Info (i.e., 3xx/4xx SIP Reason). If found, it is passed to ISDN, according to the following table: <table> <tr> <th>SIP Reason Code</th><th>ISDN Redirecting Reason</th></tr> <tr> <td>302 - Moved Temporarily</td><td>Call Forward Universal (CFU)</td></tr> <tr> <td>408 - Request Timeout</td><td rowspan="2">Call Forward No Answer (CFNA)</td></tr> <tr> <td>480 - Temporarily Unavailable</td></tr> <tr> <td>486 - Busy Here</td><td rowspan="2">Call Forward Busy (CFB)</td></tr> <tr> <td>600 - Busy Everywhere</td></tr> </table> <ul style="list-style-type: none"> If history reason is a Q.850 reason, it is translated to the SIP reason (according to the SIP-ISDN tables) and then to ISDN Redirect reason according to the table above. <p>UAS Behavior:</p> <ul style="list-style-type: none"> History-Info is sent in the final response only. Upon receiving a request with History-Info, the UAS checks the policy in the request. If 'session', 'header', or 'history' policy tag is found, the (final) response is sent without History-Info. Otherwise, it is copied from the request. | SIP Reason Code | ISDN Redirecting Reason | 302 - Moved Temporarily | Call Forward Universal (CFU) | 408 - Request Timeout | Call Forward No Answer (CFNA) | 480 - Temporarily Unavailable | 486 - Busy Here | Call Forward Busy (CFB) | 600 - Busy Everywhere |
| SIP Reason Code | ISDN Redirecting Reason | | | | | | | | | | |
| 302 - Moved Temporarily | Call Forward Universal (CFU) | | | | | | | | | | |
| 408 - Request Timeout | Call Forward No Answer (CFNA) | | | | | | | | | | |
| 480 - Temporarily Unavailable | | | | | | | | | | | |
| 486 - Busy Here | Call Forward Busy (CFB) | | | | | | | | | | |
| 600 - Busy Everywhere | | | | | | | | | | | |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|--|--|
| Use Source Number as Display Name [UseSourceNumberAsDisplay] | <p>Applicable to Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [0] No = The Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name (if Tel Display Name is received). If no Display Name is received from the Tel side, the IP Display Name remains empty (default). ▪ [1] Yes = If a Tel Display Name is received, the Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name. If no Display Name is received from the Tel side, the Tel Source Number is used as the IP Source Number and also as the IP Display Name. ▪ [2] Overwrite = The Tel Source Number is used as the IP Source Number and also as the IP Display Name (even if the received Tel Display Name is not empty). |
| Use Display Name as Source Number [UseDisplayNameAsSource] | <p>Applicable to IP-to-Tel calls.</p> <ul style="list-style-type: none"> ▪ [0] No = The IP Source Number is used as the Tel Source Number and the IP Display Name is used as the Tel Display Name (if IP Display Name is received). If no Display Name is received from IP, the Tel Display Name remains empty (default). ▪ [1] Yes = If an IP Display Name is received, it is used as the Tel Source Number and also as the Tel Display Name, the Presentation is set to Allowed (0). If no Display Name is received from IP, the IP Source Number is used as the Tel Source Number and the Presentation is set to Restricted (1). <p>For example: When the following is received 'from: 100 <sip:200@201.202.203.204>', the outgoing Source Number and Display Name are set to '100' and the Presentation is set to Allowed (0). When the following is received 'from: <sip:100@101.102.103.104>', the outgoing Source Number is set to '100' and the Presentation is set to Restricted (1).</p> |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|--|--|
| Play Ringback Tone to IP [PlayRBTone2IP] | <ul style="list-style-type: none"> [0] Don't Play = Ringback tone isn't played to the IP side of the call (default). [1] Play = Ringback tone is played to the IP side of the call after SIP 183 session progress response is sent (for analog interfaces, this applies only to FXS modules; in FXO modules the Ringback tone isn't played). <p>For digital modules: If configured to 1 ('Play'), and if EnableEarlyMedia = 1, for IP-to-Tel calls the gateway may play a ringback tone to IP, according to the following:</p> <ul style="list-style-type: none"> For CAS interfaces, the gateway opens a voice channel, sends a 183+SDP response and plays a Ringback tone to IP. For ISDN interfaces, if a Progress or an Alert message with PI (1 or 8) is received from the ISDN, the gateway opens a voice channel, sends a 183+SDP or 180+SDP response, but it doesn't play a Ringback tone to IP. If PI (1 or 8) is received from the ISDN, the gateway assumes that Ringback tone is played by the ISDN Switch. Otherwise, the gateway plays a Ringback tone to IP after receiving an Alert message from the ISDN. It sends a 180+SDP response, signaling to the originating party to open a voice channel to hear the played Ringback tone. <p>Notes:</p> <ul style="list-style-type: none"> To enable the gateway to send a 183/180+SDP responses, set EnableEarlyMedia to 1. If EnableDigitDelivery = 1, the gateway doesn't play a Ringback tone to IP and doesn't send 183 or 180+SDP responses. |
| Play Ringback Tone to Tel [PlayRBTone2Tel] | <ul style="list-style-type: none"> Determines the method used to play Ringback tone to the Tel side. [0] Don't Play = Ringback Tone isn't played. [1] Play Local = Ringback Tone is played to the Tel side of the call when 180/183 response is received. [2] Play According to Early Media = Ringback Tone is played to the Tel side of the call if no SDP is received in 180/183 responses. If 180/183 with SDP message is received, the gateway cuts through the voice channel and doesn't play Ringback tone (default). |
| Use Tgrp Information [UseSIPtgrp] | <ul style="list-style-type: none"> [0] Disable = Tgrp parameter isn't used (default). [1] Send Only = The trunk group number is added as the 'tgrp' parameter to the Contact header of outgoing SIP messages. If a trunk group number is not associated with the call, the 'tgrp' parameter isn't included. If a 'tgrp' value is specified in incoming messages, it is ignored. [2] Send and Receive = The functionality of outgoing SIP messages is identical to the functionality described in option (1). In addition, for incoming SIP messages, if the Request-URI includes a 'tgrp' parameter, the gateway routes the call according to that value (if possible). If the Contact header includes a 'tgrp' parameter, it is copied to the corresponding outgoing messages in that dialog. |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|---|--|
| Enable GRUU [EnableGRUU] | <p>Determines whether or not the Globally Routable User Agent URIs (GRUU) mechanism is used. Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default) ▪ [1] Enable = Enable <p>The gateway obtains a GRUU by generating a normal REGISTER request. This request contains a Supported header field with the value "gruu". The gateway includes a "+sip.instance" Contact header field parameter for each contact for which the GRUU is desired. This Contact parameter contains a globally unique ID that identifies the gateway instance.</p> <p>The global unique id is as follows:</p> <ul style="list-style-type: none"> ▪ If registration is per endpoint (AuthenticationMode=0), it is the MAC address of the gateway concatenated with the phone number of the endpoint. ▪ If the registration is per gateway (AuthenticationMode=1) it is only the MAC address. ▪ When the "User Information" mechanism is used, the globally unique ID is the MAC address concatenated with the phone number of the endpoint (defined in the User-Info file). <p>If the Registrar/Proxy supports GRUU, the REGISTER responses contain the "gruu" parameter in each Contact header field. The Registrar/Proxy provides the same GRUU for the same AOR and instance-id in case of sending REGISTER again after expiration of the registration. The gateway places the GRUU in any header field which contains a URI. It uses the GRUU in the following messages: INVITE requests, 2xx responses to INVITE, SUBSCRIBE requests, 2xx responses to SUBSCRIBE, NOTIFY requests, REFER requests, and 2xx responses to REFER.</p> <p>Note: If the GRUU contains the "opaque" URI parameter, the gateway obtains the AOR for the user by stripping the parameter. The resulting URI is the AOR. For example: AOR: sip:alice@example.com GRUU: sip:alice@example.com;opaque="kjh29x97us97d"</p> |
| User-Agent Information [UserAgentDisplayInfo] | <p>Defines the string that is used in the SIP request header 'User-Agent' and SIP response header 'Server'. If not configured, the default string 'AudioCodes product-name s/w-version' is used (e.g., User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.4.80.004.008). When configured, the string 'UserAgentDisplayInfo s/w-version' is used (e.g., User-Agent: MyNewOEM/v.4.80.004.008). Note that the version number can't be modified. The maximum string length is 50 characters.</p> |
| SDP Session Owner [SIPSDPSessionOwner] | <p>Determines the value of the Session Owner line ("o" field) in outgoing SDP bodies. The valid range is a string of up to 39 characters. The default value is 'AudiocodesGW'. For example: o=AudiocodesGW 1145023829 1145023705 IN IP4 10.33.4.126</p> |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|--|--|
| Play Busy Tone to Tel [PlayBusyTone2ISDN] | <p>Enables the ISDN gateway to play a Busy or a Reorder tone to the PSTN after a call is released.</p> <ul style="list-style-type: none"> [0] Don't Play = Immediately sends an ISDN Disconnect message (default). [1] Play when Disconnecting = Sends an ISDN Disconnect message with PI=8 and plays a Busy or a Reorder tone to the PSTN (depending on the release cause). [2] Play before Disconnect = Delays the sending of an ISDN Disconnect message for TimeForReorderTone seconds and plays a Busy or a Reorder tone to the PSTN. Applicable only if the call is released from the IP before it reaches the Connect state. Otherwise, the Disconnect message is sent immediately and no tones are played. |
| Subject [SIPSubject] | <p>Defines the value of the Subject header in outgoing INVITE messages. If not specified, the Subject header isn't included (default). The maximum length of the subject is limited to 50 characters.</p> |
| Multiple Packetization Time Format [MultiPtimeFormat] | <p>Determines whether the 'mptime' attribute is included in the outgoing SDP. Valid options include:</p> <ul style="list-style-type: none"> [0] None = Disabled (default) [1] PacketCable = includes the mptime attribute in the outgoing SDP -- PacketCable-defined format <p>The 'mptime' attribute enables the gateway to define a separate Packetization period for each negotiated coder in the SDP. The 'mptime' attribute is only included if this parameter is enabled, even if the remote side includes it in the SDP offer. Upon reception, each coder receives its 'ptime' value in the following precedence:</p> <ul style="list-style-type: none"> From 'mptime' attribute. From 'ptime' attribute. Default value. |
| Enable Reason Header [EnableReasonHeader] | <p>Enables / disables the usage of the SIP Reason header.</p> <ul style="list-style-type: none"> [0] Disable. [1] Enable (default). |
| Enable Semi-Attended Transfer [EnableSemiAttendedTransfer] | <p>Determines the gateway behavior when Transfer is initiated while still in Alerting state. Valid options include:</p> <ul style="list-style-type: none"> [0] Disable = Send REFER with Replaces (default). [1] Enable = Send CANCEL, and after a 487 response is received, send REFER without Replaces. |
| 3xx Behavior [3xxBehavior] | <p>Determines the gateway's behavior when a 3xx response is received for an outgoing INVITE request. The gateway can either use the same call identifiers (CallID, branch, to and from tags) or change them in the new initiated INVITE.</p> <ul style="list-style-type: none"> [0] Forward = Use different call identifiers for a redirected INVITE message (default). [1] Redirect = Use the same call identifiers. |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description | | | | | | | | | | | | | | |
|---|--|--------------------|----------|---------|--------|-----------|--------|----------|--------|------------|------------|---------------|--------|--------|--------|
| Enable P-Charging Vector [EnablePChargingVector] | <p>Enables the addition of a P-Charging-Vector header to all outgoing INVITE messages.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default) ▪ [1] Enable = Enable | | | | | | | | | | | | | | |
| Enable VoiceMail URI [EnableVMURI] | <p>Enables or disables the interworking of target and cause for redirection from Tel to IP and vice versa, according to RFC 4468.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default). ▪ [1] Enable = Enable <p>Upon receipt of a SETUP request with redirect values, the gateway maps the Redirect phone number to the target parameter, and the Redirect number reason to the cause parameter in the Request-URI.</p> <table> <tr> <td>Redirecting Reason</td><td>>> Value</td></tr> <tr> <td>Unknown</td><td>>> 404</td></tr> <tr> <td>User busy</td><td>>> 486</td></tr> <tr> <td>No reply</td><td>>> 408</td></tr> <tr> <td>Deflection</td><td>>> 487/480</td></tr> <tr> <td>Unconditional</td><td>>> 302</td></tr> <tr> <td>Others</td><td>>> 302</td></tr> </table> <p>If the gateway receives a Request-URI that includes a target and cause parameters, the target is mapped to the redirect phone number and the cause is mapped to redirect number reason.</p> | Redirecting Reason | >> Value | Unknown | >> 404 | User busy | >> 486 | No reply | >> 408 | Deflection | >> 487/480 | Unconditional | >> 302 | Others | >> 302 |
| Redirecting Reason | >> Value | | | | | | | | | | | | | | |
| Unknown | >> 404 | | | | | | | | | | | | | | |
| User busy | >> 486 | | | | | | | | | | | | | | |
| No reply | >> 408 | | | | | | | | | | | | | | |
| Deflection | >> 487/480 | | | | | | | | | | | | | | |
| Unconditional | >> 302 | | | | | | | | | | | | | | |
| Others | >> 302 | | | | | | | | | | | | | | |
| Retransmission Parameters | | | | | | | | | | | | | | | |
| SIP T1 Retransmission Timer [msec] [SipT1Rtx] | <p>The time interval (in msec) between the first transmission of a SIP message and the first retransmission of the same message. The default is 500.</p> <p>Note: The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx. For example (assuming that SipT1Rtx = 500 and SipT2Rtx = 4000):</p> <ul style="list-style-type: none"> ▪ The first retransmission is sent after 500 msec. ▪ The second retransmission is sent after 1000 (2*500) msec. ▪ The third retransmission is sent after 2000 (2*1000) msec. ▪ The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec. | | | | | | | | | | | | | | |
| SIP T2 Retransmission Timer [msec] [SipT2Rtx] | <p>The maximum interval (in msec) between retransmissions of SIP messages. The default is 4000.</p> <p>Note: The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.</p> | | | | | | | | | | | | | | |

Table 5-8: General Parameters (Protocol Definition)

| Parameter | Description |
|--------------------------------|---|
| SIP Maximum RTX [SIPMaxRtx] | Number of UDP transmissions (first transmission plus retransmissions) of SIP messages. The range is 1 to 30. The default value is 7. |

5.5.1.2 Proxy & Registration Parameters

The **Proxy & Registration** option is used to configure parameters that are associated with Proxy and Registration.

- **To configure the Proxy & Registration parameters, take these 4 steps:**
- 1. Open the 'Proxy & Registration' parameters screen (**Protocol Management** menu > **Protocol Definition** submenu > **Proxy & Registration** option).

Figure 5-10: Proxy & Registration Screen

| Proxy & Registration | |
|---|----------------|
| Enable Proxy | Use Proxy ▾ |
| Proxy Name | |
| Proxy IP Address | 0.0.0.0 |
| First Redundant Proxy IP Address | 0.0.0.0 |
| Second Redundant Proxy IP Address | 0.0.0.0 |
| Third Redundant Proxy IP Address | 0.0.0.0 |
| Redundancy Mode | Parking ▾ |
| Proxy Load Balancing Method | Disable ▾ |
| Proxy IP List Refresh Time | 60 |
| Enable Proxy Keep Alive | Disable ▾ |
| Proxy Keep Alive Time | 60 |
| Enable Fallback to Routing Table | Disable ▾ |
| Prefer Routing Table | No ▾ |
| Use Routing Table for Host Names and Profiles | Disable ▾ |
| Always Use Proxy | Disable ▾ |
| Send All Invite to Proxy | No ▾ |
| Enable Proxy Hot-Swap | Disable ▾ |
| Enable Registration | Disable ▾ |
| Gateway Name | |
| Gateway Registration Name | |
| DNS Query Type | A-Record ▾ |
| Proxy DNS Query Type | A-Record ▾ |
| Subscription Mode | Per Endpoint ▾ |
| Use Gateway Name for OPTIONS | No ▾ |
| Number of RTX Before Hot-Swap | 3 |
| User Name | |
| Password | |
| Cnonce | Default_Cnonce |
| Authentication Mode | Per Gateway ▾ |
| Set Out-Of-Service On Registration Failure | Disable ▾ |
| Challenge Caching Mode | None ▾ |
| Mutual Authentication Mode | Optional ▾ |

2. Configure the Proxy and Registration parameters according to the following table.
3. Click the **Submit** button to save your changes, or click the **Register** or **Un-Register** buttons to save your changes and register / unregister to a Proxy / Registrar.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|--|---|
| Enable Proxy [IsProxyUsed] | <p>Enables the use of a Proxy server.</p> <ul style="list-style-type: none"> ▪ [0] Don't Use Proxy = Proxy isn't used, the internal routing table is used instead (default). ▪ [1] Use Proxy = Proxy is used. <p>If you are using a Proxy server, enter the IP address of the primary Proxy server in the 'Proxy IP address' field. If you are not using a Proxy server, you must configure the Tel to IP Routing table on the gateway (described in 'Tel to IP Routing Table' on page 134).</p> |
| Proxy parameters (these parameter fields only appear if 'Enable Proxy' is enable) | |
| Proxy Name [ProxyName] | <p>Defines the Home Proxy Domain Name. If specified, the Proxy Name is used as Request-URI in REGISTER, INVITE and other SIP messages. If not specified, the Proxy IP address is used instead.</p> |
| Proxy IP Address [ProxyIP] | <p>IP address (and optionally port number) of the primary Proxy server you are using.</p> <p>Enter the IP address as FQDN or in dotted decimal notation (e.g., 201.10.8.1). You can also specify the selected port in the format: <IP Address>:<port>.</p> <p>If you enable Proxy Redundancy (by setting EnableProxyKeepAlive = 1 or 2), the gateway can work with up to 15 Proxy servers. If there is no response from the primary Proxy, the gateway tries to communicate with the redundant Proxies. When a redundant Proxy is found, the gateway either continues working with it until the next failure occurs or reverts to the primary Proxy (refer to the 'Redundancy Mode' parameter). If none of the Proxy servers respond, the gateway goes over the list again.</p> <p>The gateway also provides real time switching (hotswap mode), between the primary and redundant proxies (IsProxyHotSwap = 1). If the first Proxy doesn't respond to INVITE message, the same INVITE message is immediately sent to the next Proxy. The same logic applies to REGISTER messages (in case that RegistrarIP is not defined).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only if you select 'Use Proxy' in the 'Enable Proxy' field. ▪ If EnableProxyKeepAlive = 1 or 2, the gateway monitors the connection with the Proxies by using keep-alive messages (OPTIONS or REGISTER). ▪ To use Proxy Redundancy, you must specify one or more redundant Proxies using multiple 'ProxyIP= <IP address>' definitions. ▪ When port number is specified (e.g., domain.com:5080), DNS NAPTR/SRV queries aren't performed, even if ProxyDNSQueryType is set to 1 or 2. |

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|---|---|
| First Redundant Proxy IP Address [ProxyIP] | <p>IP addresses of the first redundant Proxy you are using. Enter the IP address as FQDN or in dotted decimal notation (e.g., 192.10.1.255). You can also specify the selected port in the format <IP Address>:<port>.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is available only if you select 'Use Proxy' in the 'Enable Proxy' field. When port number is specified, DNS NAPTR/SRV queries aren't performed, even if ProxyDNSQueryType is set to 1 or 2. For the <i>ini</i> file, the IP address of the first redundant Proxy are defined by the second repetition of the <i>ini</i> file parameter ProxyIP. |
| Second Redundant Proxy IP Address [ProxyIP] | <p>IP addresses of the second redundant Proxy you are using. Enter the IP address as FQDN or in dotted decimal notation (e.g., 192.10.1.255). You can also specify the selected port in the format <IP Address>:<port>.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is available only if you select 'Use Proxy' in the 'Enable Proxy' field. When port number is specified, DNS NAPTR/SRV queries aren't performed, even if ProxyDNSQueryType is set to 1 or 2. For the <i>ini</i> file, the IP address of the second redundant Proxy is defined by the third repetition of the <i>ini</i> file parameter ProxyIP. |
| Third Redundant Proxy IP Address [ProxyIP] | <p>IP addresses of the third redundant Proxy you are using. Enter the IP address as FQDN or in dotted decimal notation (e.g., 192.10.1.255). You can also specify the selected port in the format <IP Address>:<port>.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is available only if you select 'Use Proxy' in the 'Enable Proxy' field. When port number is specified, DNS NAPTR/SRV queries aren't performed, even if ProxyDNSQueryType is set to 1 or 2. For the <i>ini</i> file, the IP addresses of the third redundant Proxy is defined by the fourth repetition of the <i>ini</i> file parameter ProxyIP. |
| Redundancy Mode [ProxyRedundancyMode] | <ul style="list-style-type: none"> [0] Parking = gateway continues working with the last active Proxy until the next failure (default). [1] Homing = gateway always tries to work with the primary Proxy server (switches back to the main Proxy whenever it's available). <p>Note: To use ProxyRedundancyMode, enable Keep-alive with Proxy option (EnableProxyKeepAlive = 1 or 2).</p> |

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|--|---|
| Proxy Load Balancing Method [ProxyLoadBalancingMethod] | <p>Enables the usage of the Proxy Load Balancing mechanism.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Load Balancing is disabled (default). ▪ [1] Round Robin = Round Robin. ▪ [2] Random Weights = Random Weights. <p>When Round Robin (1) algorithm is used, a list of all possible Proxy IP addresses is compiled. This list includes all entries in the ProxyIP table after necessary DNS resolutions (including NAPTR and SRV, if configured). This list can handle up to 15 entries.</p> <p>After this list is compiled, the Proxy Keep-Alive mechanism (according to EnableProxyKeepAlive and ProxyKeepAliveTime) is used to mark each entry as Offline or Online. The balancing is only performed on Proxy servers that are marked as Online.</p> <p>All outgoing messages are equally distributed across the Proxy IP list. REGISTER messages are also distributed unless a RegistrarIP is configured.</p> <p>The Proxy IP list is refreshed according to ProxyIPListRefreshTime. If a change in the order of the entries in the list occurs, all load statistics are erased and balancing starts over again.</p> <p>When Random Weights (2) algorithm is used, the outgoing requests are not distributed equally among the Proxies. The weights are received from the DNS server by using SRV records. The gateway sends the requests in such a fashion that each Proxy receives a percentage of the requests according to its assigned weight. Only single FQDN should be configured as a Proxy IP address. The Random Weights Load Balancing is not used in the following scenarios:</p> <ul style="list-style-type: none"> ▪ The ProxyIP table includes more than one entry. ▪ The only Proxy defined is an IP address and not an FQDN. ▪ SRV usage is not enabled (DNSQueryType). ▪ The SRV response includes several records with a different Priority value. |
| Proxy IP List Refresh Time [ProxyIPListRefreshTime] | <p>Defines the time interval (in seconds) between refreshes of the Proxy IP list. This parameter is used only when ProxyLoadBalancingMethod = 1. The interval range is 5 to 2,000,000. The default interval is 60.</p> |

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|---|--|
| Enable Proxy Keep Alive [EnableProxyKeepAlive] | <p>Determines whether Keep-Alive with the Proxy is enabled or disabled.</p> <ul style="list-style-type: none"> [0] Disable = Disable (default) [1] Using OPTIONS = Enable Keep alive with Proxy using OPTIONS [2] Using REGISTER = Enable Keep alive with Proxy using REGISTER <p>If EnableProxyKeepAlive = 1, SIP OPTIONS message is sent every ProxyKeepAliveTime. If EnableProxyKeepAlive = 2, SIP REGISTER message is sent every RegistrationTime. Any response from the Proxy, either success (200 OK) or failure (4xx response) is considered as if the Proxy is correctly communicating.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter must be set to 1 (OPTIONS) when Proxy redundancy is used. When EnableProxyKeepAlive = 2 (REGISTER), the homing redundancy mode is disabled. When the active proxy doesn't respond to INVITE messages sent by the gateway, the proxy is marked as offline. The behavior is similar to a Keep-Alive (OPTIONS or REGISTER) failure. |
| Proxy Keep Alive Time [ProxyKeepAliveTime] | <p>Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages.</p> <p>The default value is 60 seconds.</p> <p>Note: This parameter is applicable only if EnableProxyKeepAlive = 1 (OPTIONS). When EnableProxyKeepAlive = 2 (REGISTER), the time interval between Keep-Alive messages is determined by the parameter RegistrationTime.</p> |
| Enable Fallback to Routing Table [IsFallbackUsed] | <ul style="list-style-type: none"> [0] Disable = gateway fallback is not used (default). [1] Enable = Internal Tel to IP Routing table is used when Proxy servers are unavailable. <p>When the gateway falls back to the internal Tel to IP Routing table, the gateway continues scanning for a Proxy. When the gateway finds an active Proxy, it switches from internal routing back to Proxy routing.</p> <p>Note: To enable the redundant Proxies mechanism set EnableProxyKeepAlive to 1 or 2.</p> |
| Prefer Routing Table [PreferRouteTable] | <p>Determines if the local Tel to IP routing table takes precedence over a Proxy for routing calls.</p> <ul style="list-style-type: none"> [0] No = Only Proxy is used to route calls (default). [1] Yes = The gateway checks the 'Dest Phone Prefix' and/or 'Source Phone Prefix' field in the 'Tel to IP Routing' table for a match with the outgoing call. Only if a match is not found, a Proxy is used. <p>Note: Applicable only if Proxy is not always used (AlwaysSendToProxy = 0, SendInviteToProxy = 0).</p> |

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|---|--|
| Use Routing Table for Host Names and Profiles [AlwaysUseRouteTable] | <p>Use the internal Tel to IP routing table to obtain the URI Host name and (optionally) an IP profile (per call), even if Proxy server is used.</p> <ul style="list-style-type: none"> [0] Disable = Don't use (default). [1] Enable = Use. <p>Note: This domain name is used, instead of Proxy name or Proxy IP address, in the INVITE SIP URI.</p> |
| Always Use Proxy [AlwaysSendToProxy] | <ul style="list-style-type: none"> [0] Disable = Use standard SIP routing rules (default). [1] Enable = All SIP messages and Responses are sent to Proxy server. <p>Note: Applicable only if Proxy server is used (i.e., IsProxyUsed = 1).</p> |
| Send All INVITE to Proxy [SendInviteToProxy] | <ul style="list-style-type: none"> [0] No = INVITE messages, generated as a result of Transfer or Redirect, are sent directly to the URI (according to the Refer-To header in the REFER message or Contact header in 30x response) (default). [1] Yes = All INVITE messages, including those generated as a result of Transfer or Redirect are sent to Proxy. <p>Note: Applicable only if Proxy server is used and AlwaysSendtoProxy = 0.</p> |
| Enable Proxy Hot-Swap [IsProxyHotSwap] | <p>Enable Proxy Hot-Swap redundancy mode.</p> <ul style="list-style-type: none"> [0] Disable = Disabled (default). [1] Enable = Enabled. <p>If Hot Swap is enabled, SIP INVITE/REGISTER message is first sent to the primary Proxy/Registrar server. If there is no response from the primary Proxy/Registrar server for HotSwapRtx retransmissions, the INVITE/REGISTER message is resent to the next redundant Proxy/Registrar server.</p> |
| Proxy / Registrar Registration parameters (the parameter fields appear only if 'Enable Registration' is enabled) | |
| Enable Registration [IsRegisterNeeded] | <p>Enables the gateway to register to Proxy / Registrar server.</p> <ul style="list-style-type: none"> [0] Disable = gateway doesn't register to Proxy / Registrar (default). [1] Enable = gateway registers to Proxy / Registrar when the device is powered up and every RegistrationTime seconds. <p>Note: The gateway sends a REGISTER request for each channel or for the entire gateway (according to the AuthenticationMode parameter).</p> |
| Registrar Name [RegistrarName] | <p>Registrar Domain Name. If specified, the name is used as Request-URI in REGISTER messages. If it isn't specified (default), the Registrar IP address or Proxy name or Proxy IP address is used instead.</p> |

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|--|--|
| Registrar IP Address [RegistrarIP] | <p>IP address (numerical or FQDN) and optionally port number of Registrar server.</p> <p>Enter the IP address in dotted format notation, for example, 201.10.8.1:<5080>.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ If not specified, the REGISTER request is sent to the primary Proxy server (refer to 'Proxy IP address' parameter). ▪ When port number is specified, DNS NAPTR/SRV queries aren't performed, even if DNSQueryType is set to 1 or 2. ▪ If the RegistrarIP is set to an FQDN and is resolved to multiple addresses, the gateway also provides real-time switching (hotswap mode) between different Registrar IP addresses (IsProxyHotSwap = 1). If the first Registrar doesn't respond to the REGISTER message, the same REGISTER message is immediately sent to the next Registrar. EnableProxyKeepAlive must be set to 0 in order for this logic to apply. |
| Registration Time [RegistrationTime] | <p>Defines the time (in seconds) for which registration to a Proxy server is valid. The value is used in the header 'Expires'. In addition, this parameter defines the time interval between Keep-Alive messages when EnableProxyKeepAlive = 2 (REGISTER).</p> <p>Typically, a value of 3600 should be assigned for one hour registration. The gateway resumes registration according to the parameter RegistrationTimeDivider.</p> <p>The default value is 180. The valid range is 10 to 2000000.</p> |
| Re-registration Timing [%] [RegistrationTimeDivider] | <p>Defines the re-registration timing (in percentage). The timing is a percentage of the re-register timing set by the Registration server.</p> <p>The valid range is 50 to 100. The default value is 50.</p> <p>For example: If RegistrationTimeDivider = 70 (%) and Registration Expires time = 3600, the gateway resends its registration request after 3600 x 70% = 2520 sec.</p> <p>Note: This parameter may be overridden if RegistrationTimeThreshold is greater than 0 (see description of RegistrationTimeThreshold).</p> |
| Registration Retry Time [RegistrationRetryTime] | <p>Defines the time period (in seconds) after which a Registration request is resent if registration fails with 4xx, or there is no response from the Proxy/Registrar.</p> <p>The default is 30 seconds. The range is 10 to 3600.</p> |
| Registration Time Threshold [RegistrationTimeThreshold] | <p>Defines (in seconds) a threshold for re-registration timing. If RegistrationTimeThreshold is greater than 0, but lower than the computed re-registration timing (according to RegistrationTimeDivider), the re-registration timing is set to: the timing set by the Registration server in the Expires header minus RegistrationTimeThreshold.</p> <p>The valid range is 0 to 2,000,000 seconds. The default value is 0 seconds.</p> |
| Re-register On INVITE Failure [RegisterOnInviteFailure] | <p>Enables immediate re-registration if a failure response is received for an INVITE request sent by the gateway.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default) ▪ [1] Enable = Enabled |

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|---|---|
| Miscellaneous parameters | |
| Gateway Name [SIPGatewayName] | <p>Assigns a name to the gateway (e.g., 'gateway1.com'). Ensure that the name you choose is the one that the Proxy is configured with to identify your gateway.</p> <p>Note: If specified, the gateway name is used as the host part of the SIP URI in the From header. If not specified, the gateway IP address is used instead (default).</p> |
| Gateway Registration Name [GWRegistrationName] | <p>Defines the user name that is used in the From and To headers of REGISTER messages. If GWRegistrationName isn't specified (default), the 'Username' parameter is used instead.</p> <p>Note: This parameter is applicable only to a single registration per gateway (AuthenticationMode = 1). When the gateway registers each channel separately (AuthenticationMode = 0), the user name is set to the channel's phone number.</p> |
| DNS Query Type [DNSQueryType] | <p>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to resolve Proxy and Registrar servers and to resolve all domain names that appear in the Contact and Record-Route headers.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] A-Record = A-Record (default) ▪ [1] SRV = SRV ▪ [2] NAPTR = NAPTR <p>If set to A-Record [0], no NAPTR or SRV queries are performed.</p> <p>If set to SRV [1], and the Proxy / Registrar IP address parameter, the domain name in the Contact / Record-Route headers, or the IP address defined in the Routing tables contains a domain name without port definition, an SRV query is performed. The gateway uses the first host name received from the SRV query. The gateway then performs a DNS A-record query for the host name to locate an IP address.</p> <p>If set to NAPTR [2], an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type.</p> <p>If the Proxy / Registrar IP address parameter, the domain name in the Contact / Record-Route headers, or the IP address defined in the Routing tables contains a domain name with port definition, the gateway performs a regular DNS A-record query.</p> <p>Note: To enable NAPTR/SRV queries for Proxy servers only, use the parameter ProxyDNSQueryType.</p> |

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|---|--|
| Proxy DNS Query Type [ProxyDNSQueryType] | <p>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] A-Record = A-Record (default) ▪ [1] SRV = SRV ▪ [2] NAPTR = NAPTR <p>If set to A-Record [0], no NAPTR or SRV queries are performed.</p> <p>If set to SRV [1] and the Proxy IP address parameter contains a domain name without port definition (e.g., ProxyIP = domain.com), an SRV query is performed. The SRV query returns up to four Proxy host names and their weights. The gateway then performs DNS A-record queries for each Proxy host name (according to the received weights) to locate up to four Proxy IP addresses. Therefore, if the first SRV query returns two domain names, and the A-record queries return two IP addresses each, no more searches are performed.</p> <p>If set to NAPTR [2], an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type.</p> <p>If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the gateway performs a regular DNS A-record query.</p> <p>Note: When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNSQueryType is disabled.</p> |
| Enable SRV Queries [EnableSRVQuery] | This parameter is obsolete; use the parameter DNSQueryType. |
| Enable Proxy SRV Queries [EnableProxySRVQuery] | This parameter is obsolete; use the parameter ProxyDNSQueryType. |
| Subscription Mode [SubscriptionMode] | <p>Determines the method the gateway uses to subscribe to an MWI server.</p> <ul style="list-style-type: none"> ▪ [0] Per Endpoint = Each endpoint subscribes separately. This method is typically used for FXS modules (default). ▪ [1] Per Gateway = Single subscription for the entire gateway. This method is typically used for FXO gateways. |
| Use Gateway Name for OPTIONS [UseGatewayNameForOptions] | <ul style="list-style-type: none"> ▪ [0] No = Use the gateway's IP address in keep-alive OPTIONS messages (default). ▪ [1] Yes = Use GatewayName in keep-alive OPTIONS messages. <p>The OPTIONS Request-URI host part contains either the gateway's IP address or a string defined by the parameter GatewayName. The gateway uses the OPTIONS request as a keep-alive message to its primary and redundant Proxies (EnableProxyKeepAlive = 1).</p> |

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|--|--|
| Number of RTX Before Hot-Swap [HotSwapRtx] | <p>Number of retransmitted INVITE/REGISTER messages before call is routed (hot swap) to another Proxy/Registrar. The valid range is 1 to 30. The default value is 3.</p> <p>Note: This parameter is also used for alternative routing using the Tel to IP Routing table. If a domain name in the routing table is resolved into two IP addresses, and if there is no response for HotSwapRtx retransmissions to the INVITE message that is sent to the first IP address, the gateway immediately initiates a call to the second IP address.</p> |
| User Name [UserName] | <p>This parameter is used for Registration and for Basic/Digest authentication process with a Proxy / Registrar. The parameter doesn't have a default value (empty string).</p> <p>Note 1: Applicable only if single gateway registration is used (Authentication Mode = Authentication Per gateway). Note 2: The Authentication table can be used instead.</p> |
| Password [Password] | <p>The password used for Basic/Digest authentication process with a Proxy / Registrar. Single password is used for all gateway ports. The default is 'Default_Passwd'.</p> <p>Note: The Authentication table can be used instead.</p> |
| Cnonce [Cnonce] | String used by the SIP server and client to provide mutual authentication. (Free format i.e., 'Cnonce = 0a4f113b'). The default is 'Default_Cnonce'. |
| Authentication Mode [AuthenticationMode] | <ul style="list-style-type: none"> ▪ [0] Per Endpoint = Registration and Authentication separately for each endpoint. ▪ [1] Per Gateway = Single Registration and Authentication for the entire gateway (default). ▪ [3] Per FXS Only = Registration and Authentication only for FXS endpoints. <p>Usually Authentication on a per endpoint basis is used for FXS modules, in which each endpoint registers (and authenticates) separately with its own username and password. Single Registration and Authentication (Authentication Mode = 1) is usually defined for FXO and digital modules.</p> |
| Set Out-Of-Service On Registration Failure [OOSOnRegistrationFail] | <p>Enables or disables setting an endpoint or the entire gateway (i.e., all endpoints) to out-of-service if registration fails.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enabled <p>If the registration is per endpoint (AuthenticationMode = 0) and a specific endpoint registration fails (4xx or no response), then that endpoint is set to out-of-service until a success response is received in a subsequent registration request. When the registration is per the entire gateway (AuthenticationMode = 1), and registration fails, all endpoints are set to out-of-service. The out-of-service method is set according to FXSOOSBehavior.</p> |

Table 5-9: Proxy & Registration Parameters

| Parameter | Description |
|---|---|
| Challenge Caching Mode [SIPChallengeCachingMode] | <p>Determines the mode used for Challenge Caching. Challenge Caching is used to reduce the number of SIP messages transmitted through the network. The first request to the Proxy is sent without authorization. The Proxy sends a 401/407 response with a challenge. This response is saved for further uses. A new request is resent with the appropriate credentials. Subsequent requests to the Proxy are sent with credentials (calculated from the saved challenge). If the Proxy doesn't accept the new request and sends another challenge, the old challenge is replaced with the new one.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] None = Challenges are not cached. Every new request is sent without preliminary authorization. If the request is challenged, a new request with authorization data is sent (default) ▪ [1] INVITE Only = Challenges are issued for INVITE requests are cached. This prevents a mixture of REGISTER and INVITE authorizations. ▪ [2] Full = Cache all challenges from the proxies. <p>Note: Challenge Caching is used with all proxies and not only with the active one.</p> |
| Mutual Authentication Mode [MutualAuthenticationMode] | <p>Determines the gateway's mode of operation when Authentication and Key Agreement (AKA) Digest Authentication is used.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Optional = Incoming requests that don't include AKA authentication information are accepted. ▪ [1] Mandatory = Incoming requests that don't include AKA authentication information are rejected. |

5.5.1.3 Coders

The **Coders** option allows you to configure the first to fifth preferred coders (and their attributes) for the gateway. The first coder is the highest priority coder and is used by the gateway whenever possible. If the far-end gateway cannot use the coder assigned as the first coder, the gateway attempts to use the next coder and so forth.

You can also configure the Coders table using the *ini* file parameter CoderName (refer to 'SIP Configuration Parameters' on page 323).

➤ **To configure the gateway's coders, take these 9 steps:**

1. Open the 'Coders' screen (**Protocol Management** menu > **Protocol Definition** submenu > **Coders** option).

Figure 5-11: Coders Screen

| Coders | | | | | | |
|------------|--------------------|------|--------------|---------------------|--|--|
| Coder Name | Packetization Time | Rate | Payload Type | Silence Suppression | | |
| G.711A-law | 20 | 64 | 8 | Disabled | | |
| G.723.1 | 30 | 5.3 | 4 | Disabled | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

2. From the 'Coder Name' drop-down list, select the coder you want to use. For the full list of available coders and their corresponding attributes, refer to the table below.
3. From the 'Packetization Time' drop-down list, select the packetization time (in msec) for the coder you selected. The packetization time determines how many coder payloads are combined into a single RTP packet.
4. From the 'Rate' drop-down list, select the bit rate (in kbps) for the coder you selected.
5. In the 'Payload Type' field, if the payload type for the coder you selected is dynamic, enter a value from 0 to 120 (payload types of 'well-known' coders cannot be modified). The payload type identifies the format of the RTP payload.
6. From the 'Silence Suppression' drop-down list, enable or disable the silence suppression option for the coder you selected.
7. Repeat steps 2 through 6 for the second to fifth coders (optional).
8. Click the **Submit** button to save your changes.
9. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.


Notes:

- Each coder (i.e., 'Coder Name') can appear only once.
- If packetization time and / or rate are not specified, the default value is applied.
- The ptime specifies the packetization time the gateway expects to receive. The gateway always uses the ptime requested by the remote side for sending RTP packets.
- Only the ptime of the first coder in the defined coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined.
- For G.729, it's also possible to select silence suppression without adaptations.
- If the coder G.729 is selected and silence suppression is disabled (for this coder), the gateway includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is enabled or set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception to this logic is when the remote gateway is a Cisco device (IsCiscoSCEMode).
- For an explanation on V.152 support (and implementation of T.38 and VBD coders), refer to 'Supporting V.152 Implementation' on page 387.
- A pre-defined table can be configured to provide a set of rules for automatic AMR rate change. The decision for the change is based upon packet loss rate. To obtain more information about this option, contact AudioCodes.

Table 5-10: Supported Coders

| Coder Name | Packetization Time | Rate | Payload Type | Silence Suppression |
|---|--|--|-----------------|---|
| G.711 A-law [g711Alaw64k] | 10, 20 (default), 30, 40, 50, 60, 80, 100, 120 | Always 64 | Always 8 | Disable [0] Enable [1] |
| G.711 μ-law [g711Ulaw64k] | 10, 20 (default), 30, 40, 50, 60, 80, 100, 120 | Always 64 | Always 0 | Disable [0] Enable [1] |
| G.729 [g729] | 10, 20 (default), 30, 40, 50, 60, 80, 100 | Always 8 | Always 18 | Disable [0] Enable [1] Enable w/o Adaptations [2] |
| G.723.1 [g7231] | 30 (default), 60, 90, 120 | 5.3 [0], 6.3 [1] (default) | Always 4 | Disable [0] Enable [1] |
| G.726 [g726] | 10, 20 (default), 30, 40, 50, 60, 80, 100, 120 | 16 [0], 24 [1], 32 [2] (default) 40 [3] | Dynamic (0-120) | Disable [0] Enable [1] |
| MS-GSM [gsmMS] | 40 (default) | Always 13 | Always 3 | Disable [0] Enable [1] |

Table 5-10: Supported Coders

| Coder Name | Packetization Time | Rate | Payload Type | Silence Suppression |
|--|--|--|----------------------|---------------------------|
| NetCoder [NetCoder] | 20 (default), 40, 60, 80, 100, 120 | 6.4 [0]; 7.2 [1] 8.0 [2] 8.8 [3] (default) | 51 52 53 54 | Disable [0] Enable [1] |
| G.711A-law_VBD [g711AlawVbd] | 10, 20 (default), 30, 40, 50, 60, 80, 100, 120 | Always 64 | Dynamic (0-120) | N/A |
| G.711U-law_VBD [g711UlawVbd] | 10, 20 (default), 30, 40, 50, 60, 80, 100, 120 | Always 64 | Dynamic (0-120) | N/A |
| T.38 [t38fax] | N/A | N/A | N/A | N/A |

5.5.1.4 DTMF & Dialing Parameters

The **DTMF & Dialing** option is used to configure parameters associated with dual-tone multi-frequency (DTMF) and dialing.

➤ **To configure the DTMF and dialing parameters, take these 4 steps:**

1. Open the 'DTMF & Dialing' screen (**Protocol Management** menu > **Protocol Definition** submenu > **DTMF & Dialing** option).

Figure 5-12: DTMF & Dialing Screen

| DTMF & Dialing | |
|---|---------------|
| Max Digits In Phone Num | 4 |
| Inter Digit Timeout for Overlap Dialing [sec] | 4 |
| Declare RFC 2833 in SDP | Yes |
| 1st Tx DTMF Option; | RFC 2833 |
| 2nd Tx DTMF Option; | Not Supported |
| 3rd Tx DTMF Option; | Not Supported |
| 4th Tx DTMF Option; | Not Supported |
| 5th Tx DTMF Option; | Not Supported |
| RFC 2833 Payload Type | 96 |
| Hook-Flash Option | Not Supported |
| Digit Mapping Rules | |
| Dial Tone Duration [sec] | 16 |
| Hotline Dial Tone Duration [sec] | 16 |
| Enable Special Digits | Disable |
| Default Destination Number | 1000 |
| Dial Tone Duration [sec] | 16 |
| Hotline Dial Tone Duration [sec] | 16 |
| Hook-Flash Option | Not Supported |

2. Configure the DTMF and dialing parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-11: DTMF and Dialing Parameters

| Parameter | Description |
|---|---|
| Max Digits in Phone Num [MaxDigits] | <p>Defines the maximum number of collected destination number digits that can be received (i.e., dialed) from the Tel side when Tel-to-IP overlap dialing is performed (ISDN uses overlap dialing). When the number of collected digits reaches the maximum, the gateway uses these digits for the called destination number.</p> <p>The valid range is 1 to 49. The default value is 30 for digital interfaces and 5 for analog interfaces.</p> <p>Notes:</p> <ul style="list-style-type: none"> Digit Mapping Rules can be used instead. Dialing ends when the maximum number of digits is dialed, the Interdigit Timeout expires, the '#' key is dialed, or a digit map pattern is matched. |
| Inter Digit Timeout for Overlap Dialing [sec] [TimeBetweenDigits] | <p>Defines the time (in seconds) that the gateway waits between digits that are received (i.e., dialed) from the Tel side when Tel-to-IP overlap dialing is performed (ISDN uses overlap dialing). When this inter-digit timeout expires, the gateway uses the collected digits for the called destination number.</p> <p>The valid range is 1 to 10 seconds. The default value is 4 seconds.</p> |
| Declare RFC 2833 in SDP [RxDTMFOption] | <p>Defines the supported Receive DTMF negotiation method.</p> <ul style="list-style-type: none"> [0] No = Don't declare RFC 2833 telephony-event parameter in SDP. [3] Yes = Declare RFC 2833 telephony-event parameter in SDP (default). <p>The gateway is designed to always be receptive to RFC 2833 DTMF relay packets. Therefore, it is always correct to include the 'telephony-event' parameter as a default in the SDP. However some gateways use the absence of the 'telephony-event' from the SDP to decide to send DTMF digits in-band using G.711 coder. If this is the case, you can set RxDTMFOption to 0.</p> |

Table 5-11: DTMF and Dialing Parameters

| Parameter | Description |
|---|---|
| 1 st to 5 th Tx DTMF Option [TxDTMFOption] | <p>Determines a single or several preferred transmit DTMF negotiation methods.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Not Supported = No negotiation, DTMF digits are sent according to the parameters DTMFTransportType and RFC2833PayloadType (default). ▪ [1] INFO (Nortel) = Sends DTMF digits according to IETF <draft-choudhuri-sip-info-digit-00>. ▪ [2] NOTIFY = Sends DTMF digits according to <draft-mahy-sipping-signaled-digits-01>. ▪ [3] INFO (Cisco) = Sends DTMF digits according to Cisco format. ▪ [4] RFC 2833. ▪ [5] INFO (Korea) = Sends DTMF digits according to Korea Telecom format. <p>Notes:</p> <ul style="list-style-type: none"> ▪ DTMF negotiation methods are prioritized according to the order of their appearance. ▪ When out-of-band DTMF transfer is used ([1], [2], [3], or [5]), the parameter DTMFTransportType is automatically set to 0 (DTMF digits are erased from the RTP stream). ▪ When RFC 2833 (4) is selected, the gateway: <ul style="list-style-type: none"> 1) Negotiates RFC 2833 Payload Type (PT) using local and remote SDPs. 2) Sends DTMF packets using RFC 2833 PT according to the PT in the received SDP. 3) Expects to receive RFC 2833 packets with the same PT as configured by the parameter RFC2833PayloadType. 4) Sends DTMF digits in transparent mode (as part of the voice stream). ▪ When TxDTMFOption is set to 0, the RFC 2833 PT is set according to the parameter RFC2833PayloadType for both transmit and receive. ▪ The <i>ini</i> file parameter table TxDTMFOption can be repeated 5 times for configuring the DTMF transmit methods. |
| RFC 2833 Payload Type [RFC2833PayloadType] | <p>The RFC 2833 DTMF relay dynamic payload type. Range: 96 to 99, 106 to 127; Default = 96. The 100, 102 to 105 range is allocated for proprietary usage.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ Cisco uses payload type 101 for RFC 2833. ▪ When RFC 2833 payload type (PT) negotiation is used (TxDTMFOption = 4), this payload type is used for the received DTMF packets. If negotiation isn't used, this payload type is used for receive and for transmit. |

Table 5-11: DTMF and Dialing Parameters

| Parameter | Description |
|--|---|
| Hook-Flash Option [HookFlashOption] | <p>Supported hook-flash Transport Type (method by which hook-flash is sent and received). Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Not Supported = Hook-Flash indication isn't sent (default) ▪ [1] INFO = Send proprietary INFO message with Hook-Flash indication ▪ [4] RFC 2833 <p>Notes:</p> <ul style="list-style-type: none"> ▪ FXO modules support the receiving of RFC 2833 Hook-Flash signals. ▪ The FXS modules send HookFlash signals only if EnableHold = 0. |
| Use INFO for Hook-Flash [IsHookFlashUsed] | This parameter is obsolete; use instead the parameter HookFlashOption. |
| Digit Mapping Rules [DigitMapping] | <p>Digit map pattern (used to reduce the dialing period when Overlap dialing is used). If the digit string (dialed number) has matched one of the patterns in the digit map, the gateway stops collecting digits and starts to establish a call with the collected number. The digit map pattern contains up to 52 options separated by a vertical bar (). The maximum length of the entire digit pattern is limited to 152 characters. Available notations:</p> <ul style="list-style-type: none"> ▪ [n-m] represents a range of numbers (not letters) ▪ '.' (single dot) represents repetition ▪ 'x' represents any single digit ▪ 'T' represents a dial timer (configured by TimeBetweenDigits parameter) ▪ 'S' should be used when a specific rule, that is part of a general rule, is to be applied immediately. For example, if you enter the general rule x.T and the specific rule 11x, you should append 'S' to the specific rule 11xS. <p>For example: 11xS 00T [[1-7]xxx 8xxxxxxx #xxxxxxx]*xx 91xxxxxxxxxx 9011x.T</p> <p>Note: The digitmap mechanism is applicable only when ISDN Overlap dialing is used (ISDNRxOverlap = 1).</p> |
| Dial Tone Duration [sec] [TimeForDialTone] | <p>Duration (in seconds) that the dial tone is played (for digital interface: to an ISDN terminal).</p> <p>For digital interfaces: This parameter is applicable to overlap dialing when ISDNInCallsBehavior = 65536. The dial tone is played if the ISDN Setup message doesn't include the called number. The valid range is 0 to 60. The default time is 5 seconds.</p> <p>For analog interfaces: FXS module ports play the dial tone after the phone is picked up (off hook); while FXO module ports play the dial tone after port is seized in response to ringing. The default time is 16 seconds.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ During play of dial tone, the gateway waits for DTMF digits. ▪ TimeForDialTone is not applicable when Automatic Dialing is enabled. |

Table 5-11: DTMF and Dialing Parameters

| Parameter | Description |
|---|--|
| Hotline Dial Tone Duration [HotLineToneDuration] | Duration (in seconds) of the Hotline dial tone. If no digits are received during the Hotline dial tone duration, the gateway initiates a call to a preconfigured number (set in the 'Automatic Dialing' table). The valid range is 0 to 60. The default time is 16 seconds. Note: Applicable to FXS and FXO modules. |
| Enable Special Digits [IsSpecialDigits] | <ul style="list-style-type: none"> [0] Disable = '*' or '#' terminate number collection (default). [1] Enable = if you want to allow '*' and '#' to be used for telephone numbers dialed by a user or entered for the endpoint telephone number. Note: The # and * can always be used as first digit of a dialed number, even if you select 'Disable' for this parameter. |
| Default Destination Number [DefaultNumber] | Defines the telephone number that the gateway uses if the parameter TrunkGroup doesn't include a phone number. The parameter is used as a starting number for the list of channels comprising all trunk groups in the gateway. |

5.5.2 Configuring the Advanced Parameters

The **Advanced Parameters** submenu is used to configure the gateway's advanced control protocol parameters:

- General Parameters (refer to 'General Parameters' on page [103](#))
- Supplementary Services (refer to 'Supplementary Services' on page [113](#))
- Metering Tones (refer to 'Metering Tones' on page [118](#))
- Keypad Features (refer to 'Keypad Features' on page [120](#))
- Stand-Alone Survivability (refer to 'Stand-Alone Survivability' on page [123](#))

5.5.2.1 General Parameters

The **General Parameters** option is used to configure general control protocol parameters.

➤ **To configure the advanced general protocol parameters, take these 4 steps:**

1. Open the 'General Parameters' screen (**Protocol Management** menu > **Advanced Parameters** submenu > **General Parameters** option).

Figure 5-13: General Parameters (Advanced Submenu)

| General Parameters | |
|--|------------------------|
| IP Security | Disable |
| Filter Calls to IP | Don't Filter |
| I Enable Digit Delivery to Tel | Disable |
| I Enable Digit Delivery to IP | Disable |
| RTP Only Mode | Disable |
| PSTN Alert Timeout | 180 |
| Enable DID Wink | Enable |
| Delay Before DID Wink | 0 |
| Reanswer Time | 0 |
| Disconnect and Answer Supervision | |
| Enable Polarity Reversal | Disable |
| Enable Current Disconnect | Disable |
| Disconnect on Broken Connection | Yes |
| Broken Connection Timeout [100 msec] | 100 |
| Disconnect Call on Silence Detection | No |
| Silence Detection Period [sec] | 120 |
| Silence Detection Method | Voice/Energy Detectors |
| Enable Fax Re-Routing | Disable |
| Send Digit Pattern on Connect | |
| CDR and Debug | |
| CDR Server IP Address | |
| CDR Report Level | None |
| Debug Level | 5 |
| Misc. Parameters | |
| Progress Indicator to IP | Not Configured |
| Enable X-Channel Header | Disable |
| Enable Busy Out | Disable |
| Default Release Cause | 3 |
| Delay After Reset [sec] | 7 |
| Max Number of Active Calls | 8 |
| Max Call Duration [min] | 0 |
| Enable LAN Watchdog | Disable |
| Enable Calls Cut Through | Disable |
| Enable User-Information Usage | Disable |
| Out-Of-Service Behavior | ! Reorder Tone |

2. Configure the parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-12: General Parameters (Advanced Parameters)

| Parameter | Description |
|---|---|
| IP Security [SecureCallsFromIP] | <ul style="list-style-type: none"> ▪ [0] Disable = gateway accepts all SIP calls (default). ▪ [1] Enable = gateway accepts SIP calls only from IP addresses defined in the Tel to IP Routing table (refer to 'Tel to IP Routing Table' on page 134). The gateway rejects all calls from unknown IP addresses. <p>Note: Specifying the IP address of a Proxy server in the Tel to IP Routing table enables the gateway to only accept calls originating from the Proxy server and reject all other calls.</p> |
| Filter Calls to IP [FilterCalls2IP] | <ul style="list-style-type: none"> ▪ [0] Don't Filter = Disabled (default) ▪ [1] Filter = Enabled <p>If the filter calls to IP feature is enabled, then when a Proxy is used, the gateway first checks the Tel→IP Routing table before making a call through the Proxy. If the number is not allowed (number isn't listed or a Call Restriction routing rule of IP = 0.0.0.0 is applied), the call is released.</p> |
| Enable Digit Delivery to IP [EnableDigitDelivery2IP] | <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enable digit delivery to IP. <p>The digit delivery feature enables sending DTMF digits to the destination IP address after the Tel→IP call is answered.</p> <p>To enable this feature, modify the called number to include at least one 'p' character. The gateway uses the digits before the 'p' character in the initial INVITE message. After the call is answered, the gateway waits for the required time (# of 'p' * 1.5 seconds) and then sends the rest of the DTMF digits using the method chosen (in-band or out-of-band).</p> <p>Note: The called number can include several 'p' characters (1.5 seconds pause). For example, the called number can be as follows: 1001pp699, 8888p9p300.</p> |

Table 5-12: General Parameters (Advanced Parameters)

| Parameter | Description |
|--|---|
| Enable Digit Delivery to Tel [EnableDigitDelivery] | <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enable Digit Delivery feature for the FXO/FXS gateway <p>The digit delivery feature enables sending DTMF digits to the gateway's port after the call is answered [line offhooked (FXS) or seized (FXO)]. For IP-to-Tel calls, after answering the call, the gateway plays the DTMF digits (of the called number) towards the phone line.</p> <p>For digital modules: If the called number in IP-to-Tel call includes the characters 'w' or 'p', the gateway places a call with the first part of the called number (before 'w' or 'p') , and plays DTMF digits after the call is answered. If the character 'w' is used, the gateway waits for detection of dial tone before it starts playing DTMF digits. For example, if the number '1007766p100' is defined as the called number, the gateway places a call with 1007766 as the destination number, then, after the call is answered, it waits for 1.5 seconds and plays the rest of the number (100) as DTMF digits.</p> <p>Other examples: 1664wpp102, 66644ppp503, 7774w100pp200.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The called number can include characters 'p' (1.5 seconds pause) and 'd' (detection of dial tone). If character 'd' is used, it must be the first 'digit' in the called number. The character 'p' can be used several times. For example (for FXS/FXO module), the called number can be as follows: d1005, dpp699, p9p300. To add the 'd' and 'p' digits, use the usual number manipulation rules. ▪ To use this feature with FXO modules, configure the gateway to operate in one stage dialing mode. ▪ If the parameter EnableDigitDelivery is enabled, it is possible to configure the FXS/FXO gateway to wait for dial tone per destination phone number (before or during dialing of destination phone number), therefore, the parameter IsWaitForDialTone (configurable for the entire gateway) is ignored. ▪ The FXS and digital modules send SIP 200 OK responses only after the DTMF dialing has completed. |
| RTP Only Mode [RTPOnlyMode] | <p>Enables the gateway to start sending and/or receiving RTP packets to and from remote endpoints without the need to establish a Control session. The remote IP address is determined according to the Tel to IP Routing table. The port is the same port as the local RTP port (set by BaseUDPPort and the channel on which the call was received). Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default). ▪ [1] Transmit & Receive = send and receive RTP. ▪ [2] Transmit Only= send RTP only. ▪ [3] Receive Only= receive RTP only. |

Table 5-12: General Parameters (Advanced Parameters)

| Parameter | Description |
|---|--|
| PSTN Alert Timeout [PSTNAlertTimeout] | <p>For Digital: Alert Timeout (in seconds) (ISDN T301 timer) for outgoing calls to PSTN. This timer is used between the time SETUP is sent to the Tel side (IP to Tel call establishment) and CONNECT is received. If ALERT is received, the timer is restarted.</p> <p>For Analog: Alert Timeout (in seconds) for outgoing calls to the Tel side. This timer is used between the time ring is generated (FXS) or line is seized (FXO) until the call is connected.</p> <p>The default is 180 seconds. The range is 1 to 600.</p> <p>Note: If per trunk configuration (using TrunkPSTNAlertTimeout) is set to other than default (refer to 'Trunk Settings' on page 206), the PSTNAlertTimeout parameter value is overridden.</p> |
| Enable DID Wink [EnableDIDWink] | <ul style="list-style-type: none"> [0] Disable = Direct Inward Dial (DID) is disabled (default). [1] Enable = Enable DID. <p>If enabled, the gateway can be used for connection to EIA/TIA-464B DID Loop Start lines. Both FXO (detection) and FXS (generation) are supported.</p> <p>An FXO module dials DTMF digits after a Wink signal is detected (instead of a Dial tone).</p> <p>An FXS module generates the Wink signal after the detection of offhook (instead of playing a Dial tone).</p> |
| Delay Before DID Wink [DelayBeforeDIDWink] | <p>Defines the time interval (in seconds) between detection of offhook and generation of DID Wink. Applicable only to FXS modules.</p> <p>The valid range is 0 to 1,000. The default value is 0.</p> |
| Reanswer Time [RegretTime] | <p>For Analog interfaces: The time period after user hangs up the phone and before the call is disconnected (FXS). Also called regret time.</p> <p>For Digital interfaces: Determines the time period (in seconds) the gateway waits for an MFC R2 Resume (Reanswer) signal once a Suspend (Clear back) signal was received from the PBX. If this timer expires, the call is released.</p> <p>Applicable only for MFC R2 CAS Brazil variant.</p> <p>The valid range is 0 to 255 (in seconds). The default value is 0.</p> |
| Disconnect and Answer Supervision | |
| Enable Polarity Reversal [EnableReversalPolarity] | <ul style="list-style-type: none"> [0] Disable = Disable the polarity reversal service (default). [1] Enable = Enable the polarity reversal service. <p>If the polarity reversal service is enabled, then the FXS module changes the line polarity on call answer and changes it back on call release. The FXO module sends a 200 OK response when polarity reversal signal is detected (applicable to one stage dialing only), and releases a call when a second polarity reversal signal is detected.</p> |

Table 5-12: General Parameters (Advanced Parameters)

| Parameter | Description |
|---|--|
| Enable Current Disconnect [EnableCurrentDisconnect] | <ul style="list-style-type: none"> [0] Disable = Disable the current disconnect service (default). [1] Enable = Enable the current disconnect service. <p>If the current disconnect service is enabled, the FXO releases a call when current disconnect signal is detected on its port, while the FXS module generates a 'Current Disconnect Pulse' after a call is released from IP.</p> <p>The current disconnect duration is determined by the parameter CurrentDisconnectDuration. The current disconnect threshold (FXO only) is determined by the parameter CurrentDisconnectDefaultThreshold. The frequency at which the analog line voltage is sampled is determined by the parameter TimeToSampleAnalogLineVoltage.</p> |
| Disconnect on Broken Connection [DisconnectOnBrokenConnection] | <ul style="list-style-type: none"> [0] No = Don't release the call. [1] Yes = Call is released if RTP packets are not received for a predefined timeout (default). <p>Notes:</p> <ul style="list-style-type: none"> If enabled, the timeout is set by the parameter BrokenConnectionEventTimeout, in 100 msec resolution. The default timeout is 10 seconds (BrokenConnectionEventTimeout = 100). This feature is applicable only if RTP session is used without Silence Compression. If Silence Compression is enabled, the gateway doesn't detect that the RTP connection is broken. During a call, if the source IP address (from where the RTP packets are sent) is changed without notifying the gateway, the gateway filters these RTP packets. To overcome this issue, set DisconnectOnBrokenConnection = 0; the gateway doesn't detect RTP packets arriving from the original source IP address, and switches (after 300 msec) to the RTP packets arriving from the new source IP address. |
| Broken Connection Timeout [BrokenConnectionEventTimeout] | <p>The amount of time (in 100 msec units) an RTP packet isn't received, after which a call is disconnected.</p> <p>The valid range is 1 to 1000. The default value is 100 (i.e., 10 seconds).</p> <p>Notes:</p> <ul style="list-style-type: none"> Applicable only if DisconnectOnBrokenConnection = 1. Currently, this feature works only if Silence Suppression is disabled. |
| Disconnect Call on Silence Detection [EnableSilenceDisconnect] | <ul style="list-style-type: none"> [1] Yes = The gateway disconnect calls in which silence occurs in both (call) directions for more than 120 seconds. [0] No = Call is not disconnected when silence is detected (default). <p>The silence duration can be set by the FarEndDisconnectSilencePeriod parameter (default 120).</p> <p>Note: To activate this feature set EnableSilenceCompression to 1 and FarEndDisconnectSilenceMethod to 1.</p> |
| Silence Detection Period [sec] [FarEndDisconnectSilencePeriod] | <p>Duration of silence period (in seconds) prior to call disconnection.</p> <p>The range is 10 to 28,800 (i.e., 8 hours). The default is 120 seconds.</p> |

Table 5-12: General Parameters (Advanced Parameters)

| Parameter | Description |
|---|--|
| Silence Detection Method [FarEndDisconnectSilenceMethod] | <p>Silence detection method.</p> <ul style="list-style-type: none"> [0] None = Silence detection option is disabled. [1] Packets Count = According to packet count. [2] Voice/Energy Detectors = N/A. [3] All = N/A. |
| Enable Fax Re-Routing [EnableFaxReRouting] | <p>Enables or disables re-routing of Tel-to-IP calls that are identified as fax calls.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> [0] Disable = Disabled (default). [1] Enable = Enabled. <p>If a CNG tone is detected on the Tel side of a Tel-to-IP call, a "FAX" prefix is appended to the destination number before routing and manipulations occur. Standard Tel-to-IP routing table mechanism is then used to route the call, and the destination number manipulation mechanism is used to remove the "FAX" prefix, if required.</p> <p>If the initial INVITE that is used to establish the voice call (not Fax) was already sent, a CANCEL (if not connected yet) or a BYE (if already connected) is sent to tear down the voice call.</p> |
| Send Digit Pattern on Connect [TelConnectCode] | <p>Defines a digit pattern that is sent to the Tel side after 200 OK is received from the IP side. The digit pattern is a predefined DTMF sequence that is used to indicate an answer signal (e.g., for billing purposes). Applicable only to FXS modules.</p> <p>The valid range is 1 to 8 characters.</p> |
| CDR and Debug | |
| CDR Server IP Address [CDRSyslogServerIP] | <p>Defines the destination IP address for CDR logs.</p> <p>The default value is a null string that causes the CDR messages to be sent with all Syslog messages.</p> <p>Note: The CDR messages are sent to UDP port 514 (default Syslog port).</p> |
| CDR Report Level [CDRReportLevel] | <p>Determines whether or not CDRs are sent to the Syslog server, and if enabled, at which events they are sent.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> [0] None = Call Detail Record (CDR) is not used [1] End Call = CDR is sent to the Syslog server at the end of each call. [2] Start & End Call = CDR report is sent to Syslog at the start and end of each call. [3] Connect & End Call = CDR report is sent to Syslog at connection and at the end of each call. [4] Start & Connect & End Call = CDR report is sent to Syslog at the start, at connection, and at the end of each call. <p>The CDR Syslog message complies with RFC 3161 and is identified by: Facility = 17 (local1) and Severity = 6 (Informational).</p> |

Table 5-12: General Parameters (Advanced Parameters)

| Parameter | Description |
|--|--|
| Debug Level [GwDebugLevel] | <p>Syslog logging level. One of the following debug levels can be selected:</p> <ul style="list-style-type: none"> [0] 0 = Debug is disabled (default) [1] 1 = Flow debugging is enabled [2] 2 = Flow and device interface debugging are enabled [3] 3 = Flow, device interface and stack interface debugging are enabled [4] 4 = Flow, device interface, stack interface and session manager debugging are enabled [5] 5 = Flow, device interface, stack interface, session manager and device interface expanded debugging are enabled. <p>Note: Usually set to 5 if debug traces are needed.</p> |
| Misc. Parameters | |
| Progress Indicator to IP [ProgressIndicator2IP] | <p>For Analog (FXS/FXO) modules:</p> <ul style="list-style-type: none"> [0] No PI = For Tel-to-IP calls, the gateway sends '180 Ringing' SIP response to IP after placing a call to phone (FXS) or to PBX (FXO). [1] PI = 1, [8] PI = 8: For Tel-to-IP calls, if EnableEarlyMedia = 1, the gateway sends 183 session in progress message + SDP, immediately after a call is placed to Phone/PBX. This is used to cut through the voice path, before remote party answers the call, enabling the originating party to listen to network Call Progress Tones (such as Ringback tone or other network announcements). [-1] Not Configured = Default values are used. The default for FXO modules is 1; The default for FXS modules is 0. <p>For Digital (ISDN/CAS) modules:</p> <ul style="list-style-type: none"> [-1] Not Configured = for ISDN spans, the progress indicator (PI) that is received in ISDN Proceeding, Progress and Alert messages is used as described in the options below (default). [0] No PI = For IP-to-Tel call, the gateway sends 180 Ringing SIP response to IP after receiving ISDN Alert or (for CAS) after placing a call to PBX/PSTN. [1] PI = 1, [8] PI = 8: For IP-to-Tel call, if EnableEarlyMedia = 1, the gateway sends 180 Ringing with SDP in response to an ISDN alert, or it sends a '183 session in progress' message with SDP in response to only the first received ISDN Proceeding or Progress message, after a call is placed to PBX/PSTN over the trunk. |
| Enable X-Channel Header [XChannelHeader] | <ul style="list-style-type: none"> [0] Disable = x-channel header is not used (default). [1] Enable = x-channel header is generated with trunk/B-channel information. <p>The header provides information on the E1/T1 physical trunk/B-channel on which the call is received or placed. For example 'x-channel: DS/DS1-5/22', where 'DS/DS-1' is a constant string, '5' is the trunk number, and '22' is the B-channel. This header is generated by the gateway and is sent in the following messages: INVITE and 183/180/200OK responses.</p> |

Table 5-12: General Parameters (Advanced Parameters)

| Parameter | Description |
|---|---|
| Enable Busy Out [EnableBusyOut] | <ul style="list-style-type: none"> [0] Disable = 'Busy out' feature is not used (default). [1] Enable = 'Busy out' feature is enabled. <p>When Busy Out is enabled and certain scenarios exist, the gateway performs a specific behavior: Analog gateways: A reorder tone (determined by FXSOOSBehavior) is played when the phone is offhooked. Digital gateways: If Busy out is enabled, all E1/T1 trunks are automatically put out of service by taking down the D-Channel or by sending a Service Out message for T1 PRI trunks that support these messages (NI-2, 4/5-ESS, DMS-100 and Meridian): These behaviors are performed due to one of the following scenarios:</p> <ul style="list-style-type: none"> Physically disconnected from the network (i.e., Ethernet cable is disconnected). The Ethernet cable is connected, but the gateway can't communicate with any host. Note that LAN Watch-Dog must be activated (EnableLANWatchDog = 1). The gateway can't communicate with the gatekeeper/proxy (according to the Proxy keep-alive mechanism) and no other alternative exists to send the call. <p>Notes for Analog gateways:</p> <ul style="list-style-type: none"> The FXSOOSBehavior parameter is used to control the behavior of the FXS endpoints of the gateway when a Busy Out or Graceful Lock occurs. FXO endpoints during Busy Out and Lock are inactive. Refer to LifeLineType parameter for complementary optional behavior. <p>Note: The Busy Out behavior varies between different protocol types (for Digital gateways).</p> |
| Default Release Cause [DefaultReleaseCause] | <p>Default Release Cause (to IP) for IP→Tel calls, used when the gateway initiates a call release, and if an explicit matching cause for this release isn't found, a default release cause can be configured: The default release cause is: NO_ROUTE_TO_DESTINATION (3). Other common values are: NO_CIRCUIT_AVAILABLE (34), DESTINATION_OUT_OF_ORDER (27), etc.</p> <p>Note: The default release cause is described in the Q.931 notation, and is translated to corresponding SIP 40x or 50x values. For example, 404 for 3, 503 for 34, and 502 for 27. For mapping of SIP-to-Q.931 and Q.931-to-SIP release causes, refer to 'Release Reason Mapping' on page 440.</p> |
| Delay After Reset [sec] [GWAppDelayTime] | <p>Defines the amount of time (in seconds) the gateway's operation is delayed after a reset cycle. The valid range is 0 to 45. The default value is 7 seconds.</p> <p>Note: This feature helps to overcome connection problems caused by some LAN routers or IP configuration parameters change by a DHCP Server.</p> |

Table 5-12: General Parameters (Advanced Parameters)

| Parameter | Description |
|---|---|
| Max Number of Active Calls [MaxActiveCalls] | Defines the maximum number of simultaneous active calls supported by the gateway. If the maximum number of calls is reached, new calls are not established. The default value is max available channels (no restriction on the maximum number of calls). The valid range is 1 to max number of channels. |
| Max Call Duration (min) [MaxCallDuration] | Defines the maximum call duration in minutes. If this time expires, both sides of the call are released (IP and Tel). The valid range is 0 to 35791. The default is 0 (i.e., no limitation). |
| Enable LAN Watchdog [EnableLanWatchDog] | <ul style="list-style-type: none"> ▪ [0] Disable = Disable LAN Watch-Dog (default). ▪ [1] Enable = Enable LAN Watch-Dog. <p>When LAN Watch-Dog is enabled, the gateway's overall communication integrity is checked periodically. If no communication for about 3 minutes is detected, the gateway performs a self test. If the self test succeeds, the problem is logical link down (i.e., Ethernet cable disconnected on the switch side), and the Busy Out mechanism is activated if enabled (EnableBusyOut = 1). If the self test fails, the gateway restarts to overcome internal fatal communication error. Note: Enable LAN Watchdog is relevant only if the Ethernet connection is full duplex.</p> |
| Enable Calls Cut Through [CutThrough] | <p>Enables users to receive incoming IP calls while the port is in an offhook state.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enabled. <p>If enabled, FXS modules answer the call and 'cut through' the voice channel, if there is no other active call on that port, even if the port is in offhook state. When the call is terminated (by the remote party), the gateway plays a reorder tone for TimeForReorderTone seconds and is then ready to answer the next incoming call, without onhooking the phone. The waiting call is automatically answered by the gateway when the current call is terminated (EnableCallWaiting = 1). Note: This option is applicable only to FXS modules.</p> |
| Enable User-Information Usage [EnableUserInfoUsage] | <p>Enables or disables usage of the User Information loaded to the gateway via the User Information auxiliary file.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enabled. |

Table 5-12: General Parameters (Advanced Parameters)

| Parameter | Description |
|--|--|
| Out-Of-Service Behavior [FXSOOSBehavior] | <p>Determines the behavior of FXS endpoints that are not defined (in the Endpoint Phone Number table), and the behavior of all FXS endpoints when a Busy-Out condition exists.</p> <ul style="list-style-type: none">▪ [0] None = Normal operation. No response is provided to undefined endpoints. Dial tone is played to FXS endpoints when a Busy-Out condition exists.▪ [1] Reorder Tone = The gateway plays a reorder tone to the connected phone/PBX (default).▪ [2] Polarity Reversal = The gateway reverses the polarity of the endpoint, marking it unusable (relevant, for example, to PBX DID lines). This option can't be configured on-the-fly.▪ [3] Reorder Tone + Polarity Reversal = Same as 2 and 3 combined. This option can't be configured on-the-fly.▪ [4] Current Disconnect = The gateway disconnects the current of the FXS endpoint. This option can't be configured on-the-fly. |

5.5.2.2 Supplementary Services

The **Supplementary Services** option is used to configure parameters that are associated with supplementary services. For detailed information on supplementary services, refer to 'Working with Supplementary Services' on page 415.

- **To configure the supplementary services' parameters, take these 4 steps:**
- 1. Open the 'Supplementary Services' screen (**Protocol Management** menu > **Advanced Parameters** submenu > **Supplementary Services** option).

Figure 5-14: Supplementary Services Screen

| Supplementary Services | |
|---------------------------------------|---|
| Enable Hold | Enable <input type="button" value="v"/> |
| Hold Format | 0.0.0.0 <input type="button" value="v"/> |
| Call Hold Reminder Ring Timeout | 30 |
| Enable Transfer | Enable <input type="button" value="v"/> |
| Transfer Prefix | |
| Enable Call Forward | Enable <input type="button" value="v"/> |
| Enable Call Waiting | Enable <input type="button" value="v"/> |
| Number of Call Waiting Indications | 4 |
| Time Between Call Waiting Indications | 10 |
| Time Before Waiting Indication | 0 |
| Waiting Beep Duration | 300 |
| Enable Caller ID | Disable <input type="button" value="v"/> |
| Caller ID Type | Bellcore <input type="button" value="v"/> |
| Hook-Flash Code | |
| MWI Parameters | |
| Enable MWI | Disable <input type="button" value="v"/> |
| MWI Analog Lamp | Disable <input type="button" value="v"/> |
| MWI Display | Disable <input type="button" value="v"/> |
| Subscribe to MWI | No <input type="button" value="v"/> |
| MWI Server IP Address | |
| MWI Subscribe Expiration Time | 7200 |
| MWI Subscribe Retry Time | 120 |
| Stutter Tone Duration | 2000 |
| Conference | |
| ! Enable 3-Way Conference | Disable <input type="button" value="v"/> |
| Establish Conference Code | ! |
| Conference ID | conf |

- 2. Configure the supplementary services parameters according to the table below.

3. Click the **Submit** button to save your changes, or click the **Subscribe to MWI** or **Unsubscribe to MWI** buttons to save your changes and to subscribe / unsubscribe to the MWI server.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-13: Supplementary Services Parameters

| Parameter | Description |
|--|--|
| Enable Hold [EnableHold] | <p>Enables interworking of the Hold/Retrieve supplementary service from PRI to SIP.</p> <ul style="list-style-type: none"> [0] Disable = Disables. [1] Enable = Enables (default). <p>For analog: If the Hold service is enabled, a user can activate Hold (or Unhold) using the hook-flash. On receiving a Hold request, the remote party is put on-hold and hears the hold tone.</p> <p>Notes:</p> <ul style="list-style-type: none"> This capability is only supported for QSIG and Euro ISDN variants. To support interworking of the Hold/Retrieve supplementary service from SIP to ISDN, set EnableHold2ISDN = 1. To use this service, the analog gateways at both ends must support this option. |
| Hold Format [HoldFormat] | <p>Determines the format of the hold request.</p> <ul style="list-style-type: none"> [0] 0.0.0.0 = The connection IP address in SDP is 0.0.0.0 (default). [1] Send Only = The last attribute of the SDP contains the following 'a=sendonly'. |
| Call Hold Reminder Ring Timeout [CHRRTIMEOUT] | <p>Defines the timeout (in seconds) for applying the Call Hold Reminder Ring. If a user hangs up while a call is still on hold, then the FXS module rings the extension for the time specified by this parameter. If the user picks up, the call becomes active.</p> <p>The valid range is 0 to 600 seconds. The default value is 30 seconds.</p> <p>Note: Applicable only to FXS modules.</p> |
| Enable Transfer [EnableTransfer] | <ul style="list-style-type: none"> [0] Disable = Disable the call transfer service. [1] Enable = (default). <p>If the Transfer service is enabled, the user can activate Transfer using hook-flash signaling. If this service is enabled, the remote party performs the call transfer.</p> <p>Notes:</p> <ul style="list-style-type: none"> To use this service, the gateways at both ends must support this option. To use this service, set the parameter EnableHold to 1. |
| Transfer Prefix [xferPrefix] | <p>Defined string that is added, as a prefix, to the transferred / forwarded called number, when REFER / 3xx message is received.</p> <p>Notes:</p> <ul style="list-style-type: none"> The number manipulation rules apply to the user part of the 'REFER-TO / Contact' URI before it is sent in the INVITE message. The xferPrefix parameter can be used to apply different manipulation rules to differentiate transferred / forwarded number from the original dialed number. |

Table 5-13: Supplementary Services Parameters

| Parameter | Description |
|---|--|
| Enable Call Forward [EnableForward] | <ul style="list-style-type: none"> [0] Disable = Disable the Call Forward service. [1] Enable = Enable Call Forward service (using REFER) (default). <p>For FXS modules, a Call Forward table must be defined to use the Call Forward service. To define the Call Forward table, refer to Call Forward on page 157.</p> <p>Note: To use this service, the gateways at both ends must support this option.</p> |
| Enable Call Waiting [EnableCallWaiting] | <ul style="list-style-type: none"> [0] Disable = Disable the Call Waiting service. [1] Enable = Enable the Call Waiting service (default). <p>If enabled, when an FXS module receives a call on a busy endpoint, it responds with a 182 response (and not with a 486 busy). The gateway plays a call waiting indication signal. When hook-flash is detected, the gateway switches to the waiting call.</p> <p>The gateway that initiated the waiting call plays a Call Waiting Ringback tone to the calling party after a 182 response is received.</p> <p>Notes:</p> <ul style="list-style-type: none"> The gateway's Call Progress Tones file must include a Call Waiting Ringback tone (caller side) and a Call Waiting tone (called side, FXS only). The EnableHold parameter must be enabled on both the calling and the called side. You can use the <i>ini</i> file parameter table CallWaitingPerPort to enable Call Waiting per port (refer to Call Waiting on page 160). For information on the Call Waiting feature, refer to 'Call Waiting' on page 418. For information on the Call Progress Tones file, refer to the <i>SIP Series Reference Manual</i>. |
| Number of Call Waiting Indications [NumberOfWaitingIndications] | <p>Number of waiting indications that are played to the receiving side of the call (FXS only) for Call Waiting.</p> <p>The default value is 2.</p> |
| Time Between Call Waiting Indications [TimeBetweenWaitingIndications] | <p>Difference (in seconds) between call waiting indications (FXS only) for call waiting.</p> <p>The default value is 10 seconds.</p> |
| Time Before Waiting Indication [TimeBeforeWaitingIndication] | <p>Defines the interval (in seconds) before a call waiting indication is played to the port that is currently in a call (FXS only).</p> <p>The valid range is 0 to 100. The default time is 0 seconds.</p> |
| Waiting Beep Duration [WaitingBeepDuration] | <p>Duration (in msec) of waiting indications that are played to the receiving side of the call (FXS only) for Call Waiting.</p> <p>The default value is 300.</p> |

Table 5-13: Supplementary Services Parameters

| Parameter | Description |
|---|---|
| Enable Caller ID [EnableCallerID] | <ul style="list-style-type: none"> [0] Disable = Disable the Caller ID service (default). [1] Enable = Enable the Caller ID service. <p>If the Caller ID service is enabled, then, for FXS modules, calling number and Display text are sent to the gateway port. For FXO modules, the Caller ID signal is detected and sent to IP in the SIP INVITE message (as 'Display' element). For information on the Caller ID table, refer to Caller ID on page 156. To disable/enable caller ID generation per port, refer to Call Forward on page 157.</p> |
| Caller ID Type [CallerIDType] | <p>Defines one of the following standards for detection (FXO) and generation (FXS) of Caller ID, and detection (FXO) generation (FXS) of MWI (when specified) signals:</p> <ul style="list-style-type: none"> [0] Bellcore = Caller ID and MWI (default) [1] ETSI = Caller ID and MWI [2] NTT [4] Britain [16] DTMF ETSI [17] Denmark = Caller ID and MWI [18] India [19] Brazil <p>Notes:</p> <ul style="list-style-type: none"> Typically, the Caller ID signals are generated/detected between the first and second rings. However, sometimes the Caller ID is detected before the first ring signal (in such a scenario, configure RingsBeforeCallerID to 0). Caller ID detection for Britain [4] is not supported on the gateway's FXO ports. Only FXS ports can generate the Britain [4] Caller ID. To select the Bellcore Caller ID sub standard, use the parameter BellcoreCallerIDTypeOneSubStandard. To select the ETSI Caller ID substandard, use the parameter ETSICallerIDTypeOneSubStandard. To select the Bellcore MWI sub standard, use the parameter BellcoreVMWITypeOneStandard. To select the ETSI MWI sub standard, use the parameter ETSIVMWITypeOneStandard. |
| Hook-Flash Code [HookFlashCode] | <p>Determines the digit pattern used by the PBX to indicate a 'Hook-Flash' event. When this pattern is detected from the Tel side, the gateway responds as if a Hook-Flash event occurs and sends an INFO message indicating 'Hook Flash'. If configured and a Hook-Flash indication is received from the IP side, the gateway generates this pattern to the Tel side.</p> <p>The valid range is a 25-character string.</p> |

Table 5-13: Supplementary Services Parameters

| Parameter | Description |
|---|---|
| MWI Parameters | |
| Enable MWI [EnableMWI] | <p>Enable MWI (Message Waiting Indication).</p> <ul style="list-style-type: none"> [0] Disable = Disabled (default). [1] Enable = MWI service is enabled. <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only to FXS modules. The gateway supports only the reception of SIP MWI NOTIFY messages (the gateway doesn't generate these messages). For detailed information on MWI, refer to Message Waiting Indication on page 418. |
| MWI Analog Lamp [MWIAnalogLamp] | <ul style="list-style-type: none"> [0] Disable = Disable (default). [1] Enable = Enables visual Message Waiting Indication. Supplies line voltage of approximately 100 VDC to activate the phone's lamp. <p>Note: This parameter is applicable only to FXS modules.</p> |
| MWI Display [MWIDisplay] | <ul style="list-style-type: none"> [0] Disable = MWI information isn't sent to display (default). [1] Enable = MWI information is sent to display. <p>If enabled, the gateway generates an MWI FSK message that is displayed on the MWI display.</p> <p>Note: This parameter is applicable only to FXS modules.</p> |
| Subscribe to MWI [EnableMWISubscription] | <ul style="list-style-type: none"> [0] Disable = Disable MWI subscription (default). [1] Enable = Enable subscription to MWI (to MWIServerIP address). <p>Note: Use the parameter SubscriptionMode (described in Proxy & Registration Parameters on page 84) to determine whether the gateway subscribes separately per endpoint or for the entire gateway.</p> |
| MWI Server IP Address [MWIServerIP] | <p>MWI server IP address. If provided, the gateway subscribes to this IP address.</p> <p>The MWI server address can be configured as a numerical IP address or as a domain name. If not configured, the Proxy IP address is used instead.</p> |
| MWI Subscribe Expiration Time [MWIExpirationTime] | <p>MWI subscription expiration time in seconds.</p> <p>The default is 7200 seconds. The range is 10 to 72000.</p> |
| MWI Subscribe Retry Time [SubscribeRetryTime] | <p>Subscription retry time in seconds.</p> <p>The default is 120 seconds. The range is 10 to 7200.</p> |

Table 5-13: Supplementary Services Parameters

| Parameter | Description |
|---|--|
| Stutter Tone Duration [StutterToneDuration] | <p>Duration (in msec) of the played Stutter dial tone, which indicates that Call Forwarding is enabled or that there is a waiting message(s). The default is 2,000 (i.e., 2 seconds). The range is 1,000 to 60,000. The Stutter tone is played (instead of a regular Dial tone), when a Call Forward is enabled on the specific port or when MWI is received. The tone is composed of a Confirmation tone, which is played for a user-defined duration (StutterToneDuration), followed by a Stutter tone. Both tones are defined in the CPT file.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only to FXS gateways. The Message Waiting Notification (MWI) tone takes precedence over the Call Forwarding Reminder tone. For detailed information on Message Waiting Indication (MWI), refer to Message Waiting Indication on page 418. |
| Conference Parameters | |
| Enable 3-Way Conference [Enable3WayConference] | <p>Enables or disables the 3-Way Conference feature. Valid options include:</p> <ul style="list-style-type: none"> [0] Disable = Disable (default) [1] Enable = Enables 3-way conferencing |
| Establish Conference Code [ConferenceCode] | <p>Defines the digit pattern that once detected, generates the Conference-initiating INVITE when Enable3WayConference is set to 1. The valid range is a 25-character string. The default is "!" (Hook-Flash).</p> |
| Conference ID [ConferenceID] | <p>Defines the Conference Identification string (up to 16 characters). The default value is 'conf'.</p> <p>For 3-way conferencing using an external media server: The gateway uses this identifier in the Conference-initiating INVITE that is sent to the media server when Enable3WayConference is set to 1.</p> <p>When using the Mediant 1000 Media Process Module (MPM): To join a conference, the INVITE URI must include the Conference ID string, preceded by the number of the participants in the conference, and terminated by a unique number.</p> <p>For example: INVITE sip:4MyConference1234@10.1.10.10.</p> <p>INVITE messages with the same URI join the same conference.</p> <p>For example: ConferenceID = MyConference.</p> |

5.5.2.3 Metering Tones

FXS modules can generate 12/16 KHz metering pulses towards the Tel side (e.g., for connection to a payphone or private meter). Tariff pulse rate is determined according to an internal table. This capability enables users to define different tariffs according to the Source / Destination numbers and the Time-of-Day. The tariff rate includes the time interval between the generated pulses and the number of pulses generated on answer.



Note: The 'Metering Tones' screen is only available if the gateway supports FXS interfaces.

➤ **To configure the Metering Tones, take these 6 steps:**

1. Open the 'Metering Tones' screen (**Protocol Management** menu > **Advanced Parameters** submenu > **Metering Tones** option).

Figure 5-15: Metering Tones Parameters Screen

| Metering Tones | |
|-------------------------|--|
| Generate Metering Tones | Disable <input type="button" value="v"/> |
| Metering Tone Type | 12 KHz <input type="button" value="v"/> |
| Charge Codes Table | <input type="button" value="-->"/> |

2. From the 'Metering Tone Type' drop-down list, select the type of the metering tone according to your requirements (refer to the table below).
3. From the 'Generate Metering Tones' drop-down list, select the method used to configure the metering tones that are generated to the Tel side (refer to the table below). If you select 'Internal Table', you must configure the 'Charge Codes Table'. To configure the 'Charge Codes Table', refer to Charge Codes Table.
4. In the 'Tel to IP Routing' table (refer to 'Tel to IP Routing Table' on page 134), assign a charge code rule to the routing rules you require.
When a new call is established, the Tel to IP Routing table is searched for the destination IP addresses. Once a route is found, the Charge Code (configured for that route) is used to associate the route with an entry in the Charge Codes table.
5. Click the **Submit** button to save your changes.
6. To save the changes to the flash memory, refer to 'Saving Configuration' on page 278.

Table 5-14: Metering Tones Parameters

| Parameter | Description |
|---|---|
| Generate Metering Tones [PayPhoneMeteringMode] | <p>Determines the method used to configure the metering tones that are generated to the Tel side (FXS modules only).</p> <ul style="list-style-type: none"> ▪ [0] Disable = Metering tones aren't generated (default). ▪ [1] Internal Table = Metering tones are generated according to the internal table configured by the parameter ChargeCode. <p>Note: If you select 'Internal Table', you must configure the 'Charge Codes Table' (refer to 'Charge Codes Table' on page 120).</p> |
| Metering Tone Type [MeteringType] | <p>Defines the metering tone (12 kHz or 16 kHz) that is generated by FXS modules.</p> <ul style="list-style-type: none"> ▪ [0] 12 kHz = 12 kHz metering tone (default). ▪ [1] 16 kHz = 16 kHz metering tone. <p>Note: Suitable (12 kHz or 16 KHz) <i>coeff</i> must be used for FXS modules.</p> |
| Charge Codes Table | <p>For detailed information on configuring the Charge Codes Table, refer to 'Charge Codes Table' on page 120.</p> |

5.5.2.3.1 Charge Codes Table

The Charge Codes table is used to configure the metering tones (and their time interval) that the FXS modules generate to the Tel side. To associate a charge code to an outgoing Tel-to-IP call, use the 'Tel to IP Routing' table.

You can also configure the Charge Codes table using the *ini* file parameter ChargeCode (refer to 'Analog Telephony Parameters' on page 350).

➤ **To configure the Charge Codes table, take these 6 steps:**

1. Access the 'Metering Tones' screen (**Protocol Management** menu > **Advanced Parameters** submenu > **Metering Tones** option). Refer to 'Metering Tones' on page 118 to view the screen).
2. Open the 'Charge Codes Table' screen by clicking the arrow sign (-->) to the right of the Charge Codes Table label.

Figure 5-16: Charge Codes Table Screen

| Charge Codes Table | | | | | | | | | | | | |
|--------------------|---------------|---------------|------------------|---------------|---------------|------------------|---------------|---------------|------------------|---------------|---------------|------------------|
| Index | Time Period 1 | | | Time Period 2 | | | Time Period 3 | | | Time Period 4 | | |
| | End Time | Puls Interval | Pulses On Answer | End Time | Puls Interval | Pulses On Answer | End Time | Puls Interval | Pulses On Answer | End Time | Puls Interval | Pulses On Answer |
| 1 | 07 | 30 | 1 | 14 | 20 | 2 | 20 | 15 | 1 | 00 | 60 | 1 |
| 2 | 05 | 60 | 1 | 14 | 20 | 1 | 00 | 60 | 1 | | | |
| 3 | 00 | 60 | 1 | | | | | | | | | |
| 4 | | | | | | | | | | | | |

3. Use the table to define up to 25 different charge codes (each charge code is defined in a single row). Each code can include from a single and up to four different time periods in a day (24 hours). Each time period is composed of:
 - The end of the time period (in a 24 rounded-hour's format).
 - The time interval between pulses (in seconds).
 - The number of pulses sent on answer.
4. The first time period always starts at midnight (00). It is mandatory that the last time period of each rule ends at midnight (00). This prevents undefined time frames in a day. The gateway selects the time period by comparing the gateway's current time to the end time of each time period of the selected Charge Code. The gateway generates the Number of Pulses on Answer once the call is connected and from that point on, it generates a pulse each Pulse Interval. If a call starts at a certain time period and crosses to the next, the information of the next time period is used.
5. Click the **Submit** button to save your changes.
6. To save the changes to the flash memory, refer to 'Saving Configuration' on page 278.

5.5.2.4 Keypad Features

The **Keypad Features** option (applicable only to modules), enables you to activate and deactivate the following features directly from the connected telephone's keypad:

- Hotline (refer to 'Automatic Dialing' on page 155)
- Caller ID Restriction (refer to 'Caller ID' on page 156)
- Call Forward (refer to 'Call Forward' on page 157)

➤ **To configure the keypad features, take these 4 steps:**

1. Open the 'Keypad Features' screen (**Protocol Management** menu > **Advanced Parameters** submenu > **Keypad Features** option).

Figure 5-17: Keypad Features Screen

| Keypad Features | |
|------------------------------|----------------------|
| Forward | |
| Unconditional | <input type="text"/> |
| No Answer | <input type="text"/> |
| On Busy | <input type="text"/> |
| On Busy or No Answer | <input type="text"/> |
| Do Not Disturb | <input type="text"/> |
| Deactivate | <input type="text"/> |
| Caller ID Restriction | |
| Activate | <input type="text"/> |
| Deactivate | <input type="text"/> |
| Hotline | |
| Activate | <input type="text"/> |
| Deactivate | <input type="text"/> |
| Transfer | |
| Blind | <input type="text"/> |
| Call Waiting | |
| Activate | <input type="text"/> |
| Deactivate | <input type="text"/> |

2. Configure the Keypad Features according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to the flash memory, refer to 'Saving Configuration' on page 278.



Notes:

- The method used by the gateway to collect dialed numbers is identical to the method used during a regular call (i.e., max digits, interdigit timeout, digit map, etc.).
- The activation of each feature remains in effect until it is deactivated (i.e., it is not per call).

Table 5-15: Keypad Features Parameters

| Parameter | Description |
|--|---|
| Forward | |
| Note that the forward type and number can be viewed in the Call Forward Table (refer to 'Call Forward' on page 157) | |
| Unconditional [KeyCFUnCond] | Keypad sequence that activates the immediate forward option. |
| No Answer [KeyCFNoAnswer] | Keypad sequence that activates the forward on no answer option. |
| On Busy [KeyCFBusy] | Keypad sequence that activates the forward on busy option. |
| On Busy or No Answer [KeyCFBusyOrNoAnswer] | Keypad sequence that activates the forward on 'busy or no answer' option. |
| Do Not Disturb [KeyCFDoNotDisturb] | Keypad sequence that activates the Do Not Disturb option (immediately reject incoming calls). |
| To activate the required forward method from the telephone: | |
| <ol style="list-style-type: none"> 1. Dial the preconfigured sequence number on the keypad; a dial tone is heard. 2. Dial the telephone number to which the call is forwarded (terminate the number with #); a confirmation tone is heard. | |
| Deactivate [KeyCFDeact] | Keypad sequence that deactivates any of the forward options. After the sequence is pressed a confirmation tone is heard. |
| Caller ID Restriction | |
| Note that the caller ID presentation can be viewed in the Caller Display Information table (refer to 'Caller ID' on page 156) | |
| Activate [KeyCLIR] | Keypad sequence that activates the restricted Caller ID option. After the sequence is pressed a confirmation tone is heard. |
| Deactivate [KeyCLIRDeact] | Keypad sequence that deactivates the restricted Caller ID option. After the sequence is pressed a confirmation tone is heard. |
| Hotline | |
| Note that the destination phone number and the auto dial status can be viewed in the Automatic Dialing table (refer to 'Automatic Dialing' on page 155) | |
| Activate [KeyHotLine] | <p>Keypad sequence that activates the delayed hotline option.</p> <p>To activate the delayed hotline option from the telephone:</p> <ul style="list-style-type: none"> ▪ Dial the preconfigured sequence number on the keypad; a dial tone is heard. ▪ Dial the telephone number to which the phone automatically dials after a configurable delay (terminate the number with #); a confirmation tone is heard. <p>Note: Applicable only to FXS endpoints.</p> |
| Deactivate [KeyHotLineDeact] | <p>Keypad sequence that deactivates the delayed hotline option.</p> <p>After the sequence is pressed a confirmation tone is heard.</p> <p>Note: Applicable only to FXS endpoints.</p> |

Table 5-15: Keypad Features Parameters

| Parameter | Description |
|---|--|
| Transfer | |
| Blind [KeyBlindTransfer] | Keypad sequence that activates the blind transfer option. After this sequence is dialed, the current call is put on hold, a dial tone is played to the phone, and then phone number collection starts. After the phone number is collected, it's sent to the transferee in a SIP REFER request (without a Replaces header). The call is then terminated and a confirmation tone is played to the phone. If the phone number collection fails due to a mismatch, reorder tone is played to the phone. Note: Applicable only to FXS endpoints. |
| Call Waiting | |
| Note that the call waiting can be viewed in the Call Waiting table (refer to 'Call Waiting' on page 418). | |
| Activate [KeyCallWaiting] | Keypad sequence that activates the Call Waiting option. After the sequence is pressed a confirmation tone is heard. |
| Deactivate [KeyCallWaitingDeact] | Keypad sequence that deactivates the Call Waiting option. After the sequence is pressed a confirmation tone is heard. |

5.5.2.5 Stand-Alone Survivability

The **Stand-Alone Survivability** option is used to configure the SAS 'survivability' feature for Small Medium Enterprises (SME) that implement IP Centrex services. In such environments, the enterprise's incoming and outgoing telephone calls (external and internal) are controlled by the IP Centrex, which communicates with the enterprise through the WAN interface. However, to ensure call service survivability in the face of a WAN / IP or IP Centrex failure, a PSTN backup connection is provided.

This solution is provided by the gateway's integrated SAS (back-to-back User Agent) and a dedicated connection to the PSTN network. The SAS operates in one of two modes:

- **Normal Mode:** Initially, the SAS acts as a registrar so that every IP phone or residential gateway (CPE) within the SME registers to it, while it passes all registration requests to the IP Centrex. In Normal mode, the SAS functions as a statefull proxy, passing all SIP requests received from the enterprise to the IP Centrex, and vice versa. In parallel, the SAS continuously maintains a 'Keep-Alive' handshake with the IP Centrex proxy, using SIP OPTIONS or re-INVITE messages.
- **Emergency Mode:** The SAS switches to Emergency mode if it determines (from the 'Keepalive' responses) that connection with the IP Centrex is lost. This can occur due to IP Centrex server failure or WAN problems. In Emergency mode, when the IP Centrex server is down, the SAS controls all internal calls within the enterprise. In the case of outgoing calls, the SAS forwards them to the local VoIP gateway (this can be an analog FXO to PSTN or a gateway with digital E1/T1 trunk(s) to PSTN). In this way, the enterprise preserves its capability for outgoing calls.

When Emergency mode is active, the SAS continuously attempts to access the IP Centrex proxy using the regular 'Keepalive' method. After the connection is re-established, the SAS switches to pre-Normal mode. In this mode, the SAS maintains all terminations of existing calls while any new SIP call signaling (issued by new INVITE session) is transacted to/from the IP Centrex server. This requires the SAS to maintain a database of current active calls so that after releasing all calls established

during Emergency mode, the SAS can continue functioning in Normal mode. Alternatively, the SAS can be simplified by carelessly handling existing calls.

➤ **To configure the Stand-Alone Survivability parameters, take these 4 steps:**

1. Open the 'Supplementary Services' screen (**Protocol Management** menu > **Advanced Parameters** submenu > **Stand-Alone Survivability** option).

Figure 5-18: Stand-Alone Survivability Screen

| Stand-Alone Survivability | |
|---------------------------|--------|
| Enable SAS | Enable |
| ! SAS Local SIP UDP Port | 5080 |
| SAS Default Gateway IP | |

2. Configure the parameters according to the table below.
3. Click the **Submit** button to apply your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-16: Stand-Alone Survivability Parameters

| Parameter | Description |
|---|--|
| Enable SAS [EnableSAS] | <p>Enables the Stand-Alone Survivability (SAS) application. Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] Disable Disabled (default) ▪ [1] Enable = SAS Enable <p>When enabled, the gateway receives the registration requests from different SIP entities in the local network and then forwards them to the defined proxy. If the connection to the proxy fails ('Emergency Mode'), the gateway serves as a proxy, allowing calls internal to the local network or outgoing to PSTN.</p> |
| SAS Local SIP UDP Port [SASLocalSIPUDPPort] | <p>Local UDP port for sending/receiving SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port. The valid range is 1 to 65,534. The default value is 5,080.</p> |
| SAS Default Gateway IP [SASDefaultGatewayIP] | <p>The default gateway used in SAS 'Emergency Mode'. When an incoming SIP INVITE is received and the destination Address-Of-Record is not included in the SAS database, the request is immediately sent to this default gateway.</p> <p>The address can be configured as a numerical IP address or as a domain name (up to 49 characters). The default is a null string, which is interpreted as the local IP address of the gateway.</p> |

5.5.3 Configuring the Number Manipulation Tables

The VoIP gateway provides four Number Manipulation tables for incoming and outgoing calls. These tables are used to modify the destination and source telephone numbers so that the calls can be routed correctly.

The Manipulation Tables include:

- Destination Phone Number Manipulation Table for IP-to-Tel calls
- Destination Phone Number Manipulation Table for Tel-to-IP calls
- Source Phone Number Manipulation Table for IP-to-Tel calls
- Source Phone Number Manipulation Table for Tel-to-IP calls



Note: Number manipulation can occur either before or after a routing decision is made. For example, you can route a call to a specific hunt (analog module) or trunk (digital module) group according to its original number, and then you can remove / add a prefix to that number before it is routed. To control when number manipulation is done, define the IP to Tel Routing Mode (RouteModeIP2Tel), described in IP to Trunk Group Routing on page 138, and Tel to IP Routing Mode (RouteModeTel2IP) described in 'Tel to IP Routing Table' on page 134 parameters.

Possible uses for number manipulation can be as follows:

- To strip or add dialing plan digits from or to the number. For example, a user could dial 9 in front of each number to indicate an external line. This number (9) can be removed before the call is setup.
- Allow or disallow Caller ID information to be sent according to destination or source prefixes. For detailed information on Caller ID, refer to the *SIP Series Reference Manual*.
- For digital modules only: Assignment of NPI/TON to IP□Tel calls. The VoIP gateway can use a single global setting for NPI/TON classification or it can use the setting in this table on a call by call basis. Control for this is done using 'Protocol Management > Protocol Definition > Destination/Source Number Encoding Type'.

For configuring the Number Manipulation Tables, you can also use the following *ini* file parameters (refer to 'Number Manipulation and Routing Parameters' on page 359):

- NumberMapTel2IP: configures the Destination Phone Number Manipulation Table for Tel to IP Calls
- NumberMapIP2Tel: configures the Destination Phone Number Manipulation Table for IP to Tel Calls
- SourceNumberMapTel2IP: configures the Source Phone Number Manipulation Table for Tel to IP Calls
- SourceNumberMapIP2Tel: configures the Source Phone Number Manipulation Table for IP to Tel Calls

➤ **To configure the Number Manipulation tables, take these 5 steps:**

1. Open the required 'Number Manipulation' screen (**Protocol Management** menu > **Manipulation Tables** submenu); the relevant Manipulation table screen is displayed (e.g., 'Source Phone Number Manipulation Table for Tel→IP Calls' screen).

Figure 5-19: Source Phone Number Manipulation Table for Tel-to-IP Calls

| | Dest. Prefix | Source Prefix | Number of Stripped Digits | Prefix (Suffix) to Add | Number of Digits to Leave | Presentation |
|---|--------------|---------------|---------------------------|------------------------|---------------------------|----------------|
| 1 | 03 | 201 | 0 | 971 | | Allowed |
| 2 | | 1001 | 4 | 5(23) | | Restricted |
| 3 | | 123451001# | 0 | (8) | 4 | Not Configured |
| 4 | | [30-40]xx | (1) | 2 | | Not Configured |
| 5 | [6,7,8] | 2001 | 5 | 3 | | Not Configured |
| 6 | | | | | | Not Configured |

The figure above exemplifies the use of the manipulation rules in the 'Source Phone Number Manipulation Table for Tel→IP Calls':

- When destination number equals 035000 and source number equals 20155, the source number is changed to 97220155.
 - When source number equals 1001876, it is changed to 587623.
 - Source number 1234510012001 is changed to 20018.
 - Source number 3122 is changed to 2312.
2. From the 'Table Index' drop-down list, select the range of entries that you want to edit (up to 20 entries can be configured for Source Number Manipulation and 50 entries for Destination Number Manipulation).
 3. Configure the Number Manipulation table according to the table below.
 4. Click the **Submit** button to save your changes.
 5. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Notes:

- The manipulation rules are executed in the following order:
 1. Number of stripped digits.
 2. Number of digits to leave.
 3. Prefix / suffix to add.
- The manipulation rules are applied to any incoming call whose:
 1. Destination number prefix matches the prefix defined in the 'Destination Number' field.
 2. Source number prefix matches the prefix defined in the 'Source Prefix' field.
 3. Source IP address matches the IP address defined in the 'Source IP' field (if applicable).
 The number manipulation can be performed using a combination of each of the above criteria, or using each criterion independently.
- For available notations that represent multiple numbers, refer to 'Dialing Plan Notation' on page 128.



Table 5-17: Number Manipulation Parameters

| Parameter | Description |
|--|---|
| Destination Prefix | Destination (called) telephone number prefix. An asterisk (*) represents any number. |
| Source Prefix | Source (caller) telephone number prefix. An asterisk (*) represents any number. |
| Source IP (Applicable only to the 'Destination Phone Number Manipulation Table for IP to Tel') | <p>Source IP address of the call (obtained from the Contact header in the INVITE message).</p> <p>Notes:</p> <ul style="list-style-type: none"> The source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. The source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255. |
| Number of Stripped Digits | <ul style="list-style-type: none"> Remove digits from the left of the telephone number prefix: Enter the number of digits that you want removed. For example, if you enter 3 and the phone number is 5551234, the new phone number is 1234. Remove digits from the right of the telephone number prefix: Enter the number of digits in parenthesis (). <p>Note: A combination of the two options is allowed (e.g., 2(3)).</p> |
| Prefix (Suffix) to Add | <ul style="list-style-type: none"> Prefix: Enter the number or string you want added to the front of the phone number. For example, if you enter 9 and the phone number is 1234, the new number is 91234. Suffix: Enter the number or string in brackets you want added to the end of the phone number. For example, if you enter (00) and the phone number is 1234, the new number is 123400. <p>Note: You can enter a prefix and suffix in the same field (e.g., 9(00)).</p> |
| Number of Digits to Leave | Enter the number of digits that you want to retain from the right of the phone number. |
| Presentation | <ul style="list-style-type: none"> Allowed = sends Caller ID information when a call is made using these destination / source prefixes. Restricted = restricts Caller ID information for these prefixes. Not Configured = privacy is determined according to the Caller ID table (refer to 'Caller ID' on page 156). <p>Note: If 'Presentation' is set to 'Restricted' and 'Asserted Identity Mode' is set to 'P-Asserted', the From header in the INVITE message includes the following: From: 'anonymous' <sip:anonymous@anonymous.invalid> and 'privacy: id' header.</p> |

Table 5-17: Number Manipulation Parameters

| Parameter | Description |
|------------|--|
| NPI | <p>Select the Numbering Plan Indicator (NPI) assigned to this entry.</p> <ul style="list-style-type: none"> ▪ [0] Unknown (default) ▪ [9] Private ▪ [1] E.164 Public ▪ [-1] Not Configured = value received from PSTN/IP is used <p>For a detailed list of the available NPI/TON values, refer to Numbering Plans and Type of Number on page 129</p> |
| TON | <p>Select the Type of Number (TON) assigned to this entry.</p> <ul style="list-style-type: none"> ▪ If you selected 'Unknown' for the NPI, you can select Unknown [0]. ▪ If you selected 'Private' for the NPI, you can select Unknown [0], Level 2 Regional [1], Level 1 Regional [2], PISN Specific [3] or Level 0 Regional (Local) [4]. ▪ If you selected 'E.164 Public' for the NPI, you can select Unknown [0], International [1], National [2], Network Specific [3], Subscriber [4] or Abbreviated [6]. <p>The default is Unknown.</p> |

5.5.3.1 Dialing Plan Notation

The dialing plan notation applies to all the Manipulation tables as well as to the Tel to IP Routing table (refer to 'Tel to IP Routing Table' on page [134](#)) and to IP to Trunk Group Routing table (refer to IP to Trunk Group Routing on page [138](#)). The dialing notation applies to numbers entered in the 'Destination Prefix' and 'Source Prefix' fields of these tables to represent multiple numbers.

Table 5-18: Dialing Plan Notations

| Notation | Description | Example |
|--|---|---|
| [n-m] | Represents a range of numbers. (Note: range of letters is not supported.) | [5551200-5551300]#: Represents all numbers from 5551200 to 5551300. 123[100-200]#: Represents all numbers from 123100 to 123200. |
| [n,m] | Represents multiple numbers. Note: This notation only supports single-digit numbers. | [2,3,4]xxx#: Represents four-digit numbers that start with 2, 3 or 4. |
| x | Represents any single digit. | 54324: Represents any number that starts with 54324. |
| Pound sign (#) at the end of a number | Represents the end of a number. | 54324xx#: Represents a 7 digit number that starts with 54324. |
| A single asterisk (*) | Represents any number. | *: Represents any number. |

The gateway matches the rules starting at the top of the table (i.e., top rules take precedence over lower rules). For this reason, enter more specific rules above more generic rules. For example, if you enter 551 in entry 1 and 55 in entry 2, the gateway applies rule 1 to numbers that start with 551 and applies rule 2 to numbers that start with 550, 552, 553, 554, 555, 556, 557, 558 and 559. However if you enter 55 in entry 1 and 551 in entry 2, the gateway applies rule 1 to all numbers that start with 55 including numbers that start with 551.

5.5.3.2 Numbering Plans and Type of Number

Numbers are classified by their Numbering Plan Indication (NPI) and their Type of Number (TON). The gateway supports all NPI/TON classifications used in the standard. The list of ISDN ETSI NPI/TON values is shown in the following table:

Table 5-19: NPI/TON Values for ISDN ETSI

| NPI | TON | Description |
|------------------|------------------------------|--|
| Unknown [0] | Unknown [0] | A valid classification, but one that has no information about the numbering plan. |
| E.164 Public [1] | Unknown [0] | A public number in E.164 format, but no information on what kind of E.164 number. |
| | International [1] | A public number in complete international E.164 format. For example: 16135551234 |
| | National [2] | A public number in complete national E.164 format. For example: 6135551234 |
| | Subscriber [4] | A public number in complete E.164 format representing a local subscriber. For example: 5551234 |
| Private [9] | Unknown [0] | A private number, but with no further information about the numbering plan |
| | Level 2 Regional [1] | |
| | Level 1 Regional [2] | A private number with a location. For example: 3932200 |
| | PISN Specific [3] | |
| | Level 0 Regional (local) [4] | A private local extension number. For example: 2200 |

For NI-2 and DMS-100 ISDN variants, the valid combinations of TON and NPI for calling and called numbers are (Plan/Type):

- 0/0 - Unknown/Unknown
- 1/1 - International number in ISDN/Telephony numbering plan
- 1/2 - National number in ISDN/Telephony numbering plan
- 1/4 - Subscriber (local) number in ISDN/Telephony numbering plan
- 9/4 - Subscriber (local) number in Private numbering plan

5.5.3.3 Mapping NPI/TON to Phone-Context

The **Phone-Context Table** option is used to configure the mapping of NPI and TON to the Phone-Context SIP parameter. When a call is received from the ISDN/Tel, the NPI and TON are compared against the table and the Phone-Context value is used in the outgoing SIP INVITE message. The same mapping occurs when an INVITE with a Phone-Context attribute is received. The Phone-Context parameter appears in the standard SIP headers where a phone number is used (Request-URI, To, From, Diversion).

You can also configure the Phone Context table using the *ini* file parameter PhoneContext (refer to 'Number Manipulation and Routing Parameters' on page 359).

➤ **To configure the Phone-Context tables, take these 6 steps:**

1. Open the 'Phone Context Table' screen (**Protocol Management** menu > **Manipulation Tables** submenu > **Phone Context Table** option).

Figure 5-20: Phone Context Table Screen

| Phone Context Table | | | |
|-----------------------------|----------------|--------------------|------------------|
| Add Phone Context As Prefix | | Disable ▼ | |
| Phone Context Index | | 1-10 ▼ | |
| Phone Context Table | | | |
| | NPI | TON | Phone Context |
| 1 | Unknown ▼ | Unknown ▼ | unknown.com |
| 2 | Private ▼ | Level 2 Regional ▼ | host.com |
| 3 | E.164 Public ▼ | National ▼ | na.e164.host.com |
| 4 | ▼ | ▼ | |
| 5 | ▼ | ▼ | |
| 6 | ▼ | ▼ | |
| 7 | ▼ | ▼ | |
| 8 | ▼ | ▼ | |
| 9 | ▼ | ▼ | |
| 10 | ▼ | ▼ | |

2. From the 'Add Phone Context As Prefix' drop-down list, select 'Enable' to add the received Phone-Context parameter as a prefix to outgoing ISDN SETUP Called and Calling numbers, if necessary.
3. From the 'Phone Context Index' drop-down list, select the index number.
4. Configure the Phone Context table according to the table below.

5. Click the **Submit** button to save your changes.
6. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

**Notes:**

- Several rows with the same NPI-TON or Phone-Context are allowed. In such a scenario, a Tel-to-IP call uses the first match.
- Phone-Context '+' is a unique case as it doesn't appear in the Request-URI as a Phone-Context parameter. Instead, it's added as a prefix to the phone number. The '+' isn't removed from the phone number in the IP-to-Tel direction.

Table 5-20: Phone-Context Parameters

| Parameter | Description |
|---|--|
| Add Phone Context As Prefix [AddPhoneContextAsPrefix] | Determines whether or not the received Phone-Context parameter is added as a prefix to the outgoing ISDN SETUP Called and Calling numbers. Valid options include: <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default). ▪ [1] Enable = Enable. |
| NPI | Select the Number Plan assigned to this entry. You can select the following: <ul style="list-style-type: none"> ▪ [0] Unknown = Unknown (default) ▪ [1] E.164 Public = E.164 Public ▪ [9] Private = Private For a detailed list of the available NPI/TON values, refer to Numbering Plans and Type of Number on page 129. |
| TON | Select the Number Type assigned to this entry. <ul style="list-style-type: none"> ▪ If you selected Unknown as the NPI, you can select Unknown [0]. ▪ If you selected Private as the NPI, you can select Unknown [0], Level 2 Regional [1], Level 1 Regional [2], PSTN Specific [3], or Level 0 Regional (Local) [4]. ▪ If you selected E.164 Public as the NPI, you can select Unknown [0], International [1], National [2], Network Specific [3], Subscriber [4], or Abbreviated [6]. |
| Phone Context | The Phone-Context SIP URI parameter. |

5.5.4 Configuring the Routing Tables

The **Routing Tables** submenu is used to configure the gateway's IP-to-Tel and Tel-to-IP routing tables and their associated parameters:

- General Parameters (refer to 'General Parameters' on page 132)
- Tel to IP Routing Table (refer to 'Tel to IP Routing Table' on page 134)
- IP to Trunk Group Routing (refer to 'IP to Trunk Group Routing' on page 138)
- Internal DNS Table (refer to 'Internal DNS Table' on page 140)
- Internal SRV Table (refer to 'Internal SRV Table' on page 141)
- Reasons for Alternative Routing (refer to 'Reasons for Alternative Routing' on page 142)
- Release Cause Mapping (refer to 'Release Cause Mapping' on page 144)

5.5.4.1 General Parameters

The **General Parameters** option is used to configure the gateway's IP-to-Tel and Tel-to-IP routing parameters.

➤ **To configure the general routing parameters, take these 4 steps:**

1. Open the 'General Parameters' screen (**Protocol Management** menu > **Routing Tables** submenu > **General Parameters** option).

Figure 5-21: Routing Tables - General Parameters Screen

| General Parameters | | |
|---|---------|---|
| Add Trunk Group ID as Prefix | No | ▼ |
| Add Trunk ID as Prefix | No | ▼ |
| Replace Empty Destination with B-channel Phone Number | No | ▼ |
| Add NPI and TON to Called Number | No | ▼ |
| Add NPI and TON to Calling Number | No | ▼ |
| IP to Tel Remove Routing Table Prefix | No | ▼ |
| Enable Alt Routing Tel to IP | Disable | ▼ |
| Alt Routing Tel to IP Mode | None | ▼ |
| Max Allowed Packet Loss for Alt Routing [%] | 20 | |
| Max Allowed Delay for Alt Routing [msec] | 250 | |

2. Configure the general parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-21: General Parameters (Routing Tables)

| Parameter | Description |
|---|---|
| Add Trunk Group ID as Prefix [AddTrunkGroupAsPrefix] | <ul style="list-style-type: none"> [0] No = Don't add trunk group ID as prefix (default). [1] Yes = Add trunk group ID as prefix to called number. <p>If enabled, then the gateway's trunk group ID is added as a prefix to the destination phone number for Tel-to-IP calls.</p> <p>Notes:</p> <ul style="list-style-type: none"> This option can be used to define various routing rules. To use this feature, you must configure the trunk group IDs. |
| Add Trunk ID as Prefix [AddPortAsPrefix] | <ul style="list-style-type: none"> [0] No = Don't add trunk ID as prefix (default). [1] Yes = Enable add trunk ID as prefix <p>If enabled, Add trunk ID number (single digit in the range 1 to 8) as a prefix to the called (destination) phone number for Tel→IP incoming calls. This option can be used to define various routing rules.</p> |
| Replace Empty Destination with B-channel Phone Number [ReplaceEmptyDstWithPortNumber] | <ul style="list-style-type: none"> [0] No = Disabled (default). [1] Yes = Internal channel number is used as a destination number if called number is missing. <p>Note: Applicable only to Tel-to-IP calls, if called number is missing.</p> |
| Add NPI and TON to Calling Number [AddNPIandTON2CallingNumber] | <ul style="list-style-type: none"> [0] No = Do not change the Calling Number (default). [1] Yes = Add NPI and TON to the Calling Number of incoming (Tel to IP) ISDN call. <p>For example: After receiving a Calling Number = 555, NPI = 1, and TON = 3, the modified number is going to be 13555. This number can later be used for manipulation and routing purposes.</p> |
| Add NPI and TON to Called Number [AddNPIandTON2CalledNumber] | <ul style="list-style-type: none"> [0] No = Do not change the Called Number (default). [1] Yes = Add NPI and TON to the Called Number of incoming (Tel to IP) ISDN call. <p>For example: After receiving a Called Number = 555, NPI=1 and TON = 3, the modified number is now 13555. This number can later be used for manipulation and routing purposes.</p> |
| IP to Tel Remove Routing Table Prefix [RemovePrefix] | <ul style="list-style-type: none"> [0] No = Don't remove prefix (default) [1] Yes = Remove the prefix (defined in the IP to Trunk Group Routing table) from a telephone number for an IP-to-Tel call, before forwarding it to Tel. <p>For example: To route an incoming IP-to-Tel call with destination number 21100, the IP to Trunk Group Routing table is scanned for a matching prefix. If such prefix is found, 21 for instance, then before the call is routed to the corresponding trunk group, the prefix (21) is removed from the original number so that only 100 is left.</p> <p>Notes:</p> <ul style="list-style-type: none"> Applicable only if number manipulation is performed after call routing for IP→Tel calls (refer to 'IP to Tel Routing Mode' parameter -- RouteModelIP2Tel = 0). Similar operation (of removing the prefix) is also achieved by using the usual number manipulation rules. |

Table 5-21: General Parameters (Routing Tables)

| Parameter | Description |
|--|---|
| Enable Alt Routing Tel to IP [AltRoutingTel2IPEnable] | <p>Determines the operation modes for the Alternative Routing mechanism.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable the Alternative Routing feature (default). ▪ [1] Enable = Enable the Alternative Routing feature. ▪ [2] Status Only = The Alternative Routing feature is disabled and a read-only information on the quality of service of the destination IP addresses is provided. <p>For information on the Alternative Routing feature, refer to 'Configuring Alternative Routing (Based on Connectivity and QoS)' on page 398.</p> |
| Alt Routing Tel to IP Mode [AltRoutingTel2IPMode] | <ul style="list-style-type: none"> ▪ [0] None = Alternative routing is not used. ▪ [1] Connectivity = Alternative routing is performed if ping to initial destination fails. ▪ [2] QoS = Alternative routing is performed if poor Quality of Service is detected. ▪ [3] Both = Alternative routing is performed if either ping to initial destination fails, poor Quality of Service is detected, or DNS host name is not resolved (default). <p>Notes:</p> <ul style="list-style-type: none"> ▪ QoS (Quality of Service) is quantified according to delay and packet loss, calculated according to previous calls. QoS statistics are reset if no new data is received for two minutes. For information on the Alternative Routing feature, refer to 'Configuring Alternative Routing (Based on Connectivity and QoS)' on page 398. ▪ To receive quality information (displayed in the Quality Status and Quality Info. fields in 'IP Connectivity' on page 251) regarding a given destination, the parameter AltRoutingTel2IPMode must be set to 2 or 3. |
| Max Allowed Packet Loss for Alt Routing [%] [IPConnQoSMaxAllowedPL] | <p>Packet loss percentage at which the IP connection is considered a failure. The range is 1 to 20%. The default value is 20%.</p> |
| Max Allowed Delay for Alt Routing [msec] [IPConnQoSMaxAllowedDelay] | <p>Transmission delay (in msec) at which the IP connection is considered a failure. The range is 100 to 1000. The default value is 250 msec.</p> |

5.5.4.2 Tel to IP Routing Table

The Tel to IP Routing Table is used to route incoming Tel calls to IP addresses. This routing table associates a called / calling telephone number's prefixes with a destination IP address or with a Fully Qualified Domain Name (FQDN). When a call is routed through the VoIP gateway (Proxy isn't used), the called and calling numbers are compared to the list of prefixes in the IP Routing table (up to 50 prefixes can be configured); Calls that match these prefixes are sent to the corresponding IP address. If the number dialed does not match these prefixes, the call is not made.

When using a Proxy server, you do not need to configure the Tel to IP Routing Table. However, if you want to use fallback routing when communication with Proxy servers is lost, or to use the 'Filter Calls to IP' and 'IP Security' features, or to obtain different SIP URI host names (per called number) or to assign IP profiles, you need to configure the IP Routing Table.

Note that for the Tel to IP Routing table to take precedence over a Proxy for routing calls, set the parameter `PreferRouteTable` to 1. The gateway checks the 'Destination IP Address' field in the 'Tel to IP Routing' table for a match with the outgoing call. Only if a match is not found, a Proxy is used.

Possible uses for Tel to IP Routing include the following:

- Can fallback to internal routing table if there is no communication with the Proxy servers.
- Call Restriction (when Proxy isn't used): rejects all outgoing Tel→IP calls that are associated with the destination IP address: 0.0.0.0.
- IP Security: When the IP Security feature is enabled (`SecureCallFromIP` = 1), the VoIP gateway accepts only those IP→Tel calls with a source IP address identical to one of the IP addresses entered in the Tel to IP Routing Table.
- Filter Calls to IP: When a Proxy is used, the gateway checks the Tel→IP Routing table before a telephone number is routed to the Proxy. If the number is not allowed (number isn't listed or a Call Restriction routing rule is applied), the call is released.
- Always Use Routing Table: When this feature is enabled (`AlwaysUseRouteTable` = 1), even if a Proxy server is used, the SIP URI host name in the sent INVITE message is obtained from this table. Using this feature, users are able to assign a different SIP URI host name for different called and/or calling numbers.
- Assign Profiles to destination address (also when a Proxy is used).
- Alternative Routing (when Proxy isn't used): an alternative IP destination for telephone number prefixes is available. To associate an alternative IP address to called telephone number prefix, assign it with an additional entry (with a different IP address), or use an FQDN that resolves to two IP addresses. The call is sent to the alternative destination when one of the following occurs:
 - No ping to the initial destination is available, or when poor QoS (delay or packet loss, calculated according to previous calls) is detected, or when a DNS host name is not resolved. For detailed information on Alternative Routing, refer to 'Configuring Alternative Routing (Based on Connectivity and QoS)' on page 398.
 - When a release reason that is defined in the 'Reasons for Alternative Tel to IP Routing' table is received. For detailed information on the 'Reasons for Alternative Routing Tables', refer to 'Reasons for Alternative Routing' on page 142.

Alternative routing (using this table) is commonly implemented when there is no response to an INVITE message (after INVITE retransmissions). The gateway then issues an internal 408 'No Response' implicit release reason. If this reason is included in the 'Reasons for Alternative Routing' table, the gateway immediately initiates a call to the redundant destination using the next matched entry in the 'Tel to IP Routing' table. Note that if a domain name in this table is resolved to two IP addresses, the timeout for INVITE retransmissions can be reduced by using the parameter 'Number of RTX Before Hotswap'.



Note: If the alternative routing destination is the gateway itself, the call can be configured to be routed back to PSTN. This feature is referred to as 'PSTN Fallback', meaning that if sufficient voice quality is not available over the IP network, the call is routed through the legacy telephony system (PSTN).



Tip: Tel-to-IP routing can be performed either before or after applying the number manipulation rules. To control when number manipulation is performed, set the Tel to IP Routing Mode (or RouteModeTel2IP *ini* file) parameter (described in the table below).

You can also configure the Tel to IP Routing table using the *ini* file parameter Prefix (refer to 'Number Manipulation and Routing Parameters' on page 359).

➤ **To configure the Tel to IP Routing table, take these 6 steps:**

1. Open the 'Tel to IP Routing' screen (**Protocol Management** menu > **Routing Tables** submenu > **Tel to IP Routing** option).

Figure 5-22: Tel to IP Routing Screen

| Tel to IP Routing | | | | | | |
|------------------------|--------------------|---------------------|---------------------------------|------------|--------|-------------|
| Routing Index | | | 1-10 | | | |
| Tel to IP Routing Mode | | | Route calls before manipulation | | | |
| | Dest. Phone Prefix | Source Phone Prefix | Dest. IP Address | Profile ID | Status | Charge Code |
| 1 | 10 | 100 | 10.33.45.63 | 1 | n/a | 1 |
| 2 | 20 | * | 10.33.45.60 | 1 | n/a | 1 |
| 3 | [3,4,6] | * | 10.33.45.64 | 1 | n/a | 2 |
| 4 | 54324 | [1,2] | domain.com | 1 | n/a | 3 |
| 5 | 9 | * | 0.0.0.0 | 2 | | 3 |
| 6 | 8xx# | * | 10.13.77.7 | 1 | | 4 |
| 7 | | | | | | |

2. From the 'Tel to IP Routing Mode' drop-down list, select the required Tel to IP routing mode (refer to the table below).
3. From the 'Routing Index' drop-down list, select the range of entries that you want to add.
4. Configure the Tel to IP Routing table according to the table below.
5. Click the **Submit** button to save your changes.
6. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-22: Tel to IP Routing Table

| Parameter | Description |
|---|--|
| Tel to IP Routing Mode [RouteModeTel2IP] | <p>Defines the order between routing incoming calls to IP, using routing table, and manipulation of destination number.</p> <ul style="list-style-type: none"> ▪ [0] Route calls before manipulation = Tel-to-IP calls are routed before the number manipulation rules are applied (default). ▪ [1] Route calls after manipulation = Tel-to-IP calls are routed after the number manipulation rules are applied. <p>Note: Not applicable if outbound Proxy routing is used.</p> |
| Dest. Phone Prefix | Represents a called telephone number prefix. The prefix can be 1 to 19 digits long. An asterisk (*) represents all numbers. |
| Source Phone Prefix | Represents a calling telephone number prefix. The prefix can be 1 to 19 digits long. An asterisk (*) represents all numbers. |
| <p>Any telephone number whose destination number matches the prefix defined in the 'Dest. Phone Prefix' field <i>and</i> its source number matches the prefix defined in the adjacent 'Source Phone Prefix' field is sent to the IP address entered in the 'Dest. IP Address' field.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ Tel to IP routing can be performed according to a combination of source and destination phone prefixes, or using each independently. ▪ An additional entry of the same prefixes can be assigned to enable alternative routing. ▪ For available notations that represent multiple numbers, refer to 'Dialing Plan Notation' on page 128. | |
| Dest. IP Address | <p>The IP address (and optionally port number) assigned to the prefix. For example, <IP Address>:<Port>.</p> <p>Domain names such as domain.com, can be used instead of IP addresses. To discard outgoing IP calls, enter 0.0.0.0.</p> <p>Note: When using domain names, you must enter a DNS server IP address or alternatively, define these names in the 'Internal DNS Table'.</p> |
| Profile ID | IP profile number assigned to the destination IP address that is defined in the 'Dest. IP Address' field. |
| Status | <p>A read-only field representing the Quality of Service of the destination IP address:</p> <ul style="list-style-type: none"> ▪ n/a = Alternative Routing feature is disabled. ▪ OK = IP route is available ▪ Ping Error = No ping to IP destination; route is not available ▪ QoS Low = Bad QoS of IP destination; route is not available ▪ DNS Error = No DNS resolution (only when domain name is used instead of an IP address). |
| Charge Code | An optional Charge Code (1 to 25) can be applied to each routing rule to associate it with an entry in the Charge Code table (refer to Charge Codes Table on page 120). |

5.5.4.3 IP to Trunk Group Routing

The IP to Trunk Group Routing Table is used to route incoming IP calls to groups of channels (for digital modules, these are E1/T1 B-channels) called trunk groups. Calls are assigned to trunk groups according to any combination of the following three options (or using each independently):

- Destination phone prefix
- Source phone prefix
- Source IP address

The call is then sent to the VoIP gateway channels assigned to that trunk group. The specific channel, within a trunk group that is assigned to accept the call is determined according to the trunk group's channel selection mode which is defined in the 'Trunk Group Settings' screen (refer to 'Configuring the Trunk Group Settings' on page 152) or according to the global parameter ChannelSelectMode (refer to 'Number Manipulation and Routing Parameters' on page 359). Trunk groups can be used on both FXO and FXS modules; however, they are typically used with FXO modules.



Note: When a release reason that is defined in the 'Reasons for Alternative IP to Tel Routing' table is received for a specific IP→Tel call, an alternative Trunk Group for that call is available. To associate an alternative Trunk Group to an incoming IP call, assign it with an additional entry in the 'IP to Trunk Group Routing' table (repeat the same routing rules with a different Trunk Group ID). For detailed information on the 'Reasons for Alternative Routing Tables', refer to 'Reasons for Alternative Routing' on page 142.

To use Trunk Groups you must also perform the following:

- Assign a Trunk Group ID to the VoIP gateway's channels in the 'Trunk Group Table' screen. For information on how to assign a Trunk Group ID to a channel, refer to 'Configuring the Trunk Group Table' on page 150.
- You can configure the 'Trunk Group Settings' table to determine the method in which new calls are assigned to channels within the Trunk Groups (a different method for each Trunk Group can be configured). For information on how to enable this option, refer to 'Configuring the Trunk Group Settings' on page 152. If a Channel Select Mode for a specific Trunk Group isn't specified, then the global Channel Select Mode parameter (defined in the 'General Parameters' screen under 'Advanced Parameters') applies.

You can also configure the IP to Trunk Group Routing table using the *ini* file parameter PSTNPrefix (refer to 'Number Manipulation and Routing Parameters' on page 359).

➤ **To configure the IP to Trunk Group Routing table, take these 6 steps:**

1. Open the 'IP to Trunk Group Routing' screen (**Protocol Management** menu > **Routing Tables** submenu > **IP to Trunk Group Routing** option).

Figure 5-23: IP to Trunk Group Routing Table Screen

| IP to Trunk Group Routing Table | | | | | |
|---------------------------------|--------------------|---------------------|-----------------------------------|----------------|------------|
| Routing Index | | | 1-12 ▼ | | |
| IP To Tel Routing Mode | | | Route calls before manipulation ▼ | | |
| | Dest. Phone Prefix | Source Phone Prefix | Source IP Address | Trunk Group ID | Profile ID |
| 1 | 10 | * | 0 | 1 | 2 |
| 2 | 20 | 101 | 0 | 1 | 2 |
| 3 | [5010-5020] | * | 0 | 3 | 1 |
| 4 | 6xx | * | 0 | 3 | 1 |
| 5 | 71234# | * | 0 | 3 | 1 |
| 6 | * | * | 0 | 4 | 3 |
| 7 | | | | | |

2. From the 'IP to Tel Routing Mode' field, select the IP to Tel routing mode (refer to the table below).
3. From the 'Routing Index' drop-down list, select the range of entries that you want to add. Up to 24 entries can be configured.
4. Configure the 'IP to Trunk Group Routing' table according to the table below.
5. Click the **Submit** button to save your changes.
6. To save the changes so they are available after a power fail, refer to 'Saving Configuration' on page 278.

Table 5-23: IP to Trunk Group Routing Table

| Parameter | Description |
|--|---|
| IP to Tel Routing Mode [RouteModelIP2Tel] | Defines order between routing calls to Trunk group and manipulation of destination number. <ul style="list-style-type: none"> ▪ [0] Route calls before manipulation = IP-to-Tel calls are routed before the number manipulation rules are applied (default). ▪ [1] Route calls after manipulation = IP-to-Tel calls are routed after the number manipulation rules are applied. |
| Dest. Phone Prefix | Represents a called telephone number prefix. The prefix can be 1 to 49 digits long. An asterisk (*) represents all numbers. |
| Source Phone Prefix | Represents a calling telephone number prefix. The prefix can be 1 to 49 digits long. An asterisk (*) represents all numbers. |

Table 5-23: IP to Trunk Group Routing Table

| Parameter | Description |
|--|---|
| Source IP Address | Represents the source IP address of an IP-to-Tel call (obtained from the Contact header in the INVITE message). Note: The source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. In addition, the source IP address can include the asterisk (*) wildcard, which represents any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255. |
| Any SIP incoming call whose destination number matches the prefix defined in the 'Dest. Phone Prefix' field, <i>and</i> whose source number matches the prefix defined in the adjacent 'Source Phone Prefix' field, <i>and</i> whose source IP address matches the address defined in the 'Source IP Address' field is assigned to the Trunk Group in the corresponding 'Trunk Group ID' field. Notes: <ul style="list-style-type: none"> IP-to-Trunk Group routing can be performed according to any combination of source / destination phone prefixes and source IP address, or using each independently. For available notations that represent multiple numbers (used in the prefix columns), refer to 'Dialing Plan Notation' on page 128. | |
| Trunk Group ID | Trunk Group ID to which calls that match these prefixes are assigned. |
| Profile ID | Number of the IP profile that is assigned to the routing rule. |

5.5.4.4 Internal DNS Table

The **Internal DNS Table** option, similar to a DNS resolution, is used to translate host names into IP addresses. It is used when hostname translation is required (e.g., 'Tel to IP Routing' table). Two different IP addresses can be assigned to the same hostname. If the hostname isn't found in this table, the gateway communicates with an external DNS server.

Assigning two IP addresses to hostname can be used for alternative routing (using the 'Tel to IP Routing' table).

For a description of the *ini* file parameter DNS2IP used to configure the Internal DNS table, refer to 'Networking Parameters' on page 299.



Note: If the Internal DNS table is configured, the gateway first tries to resolve a domain name using this table. If the domain name isn't found, the gateway performs a DNS resolution using an external DNS server.

➤ **To configure the internal DNS table, take these 7 steps:**

1. Open the 'Internal DNS Table' screen (**Protocol Management** menu > **Routing Tables** submenu > **Internal DNS Table** option).

Figure 5-24: Internal DNS Table Screen

| Internal DNS Table | | | |
|--------------------|----------------|------------------|-------------------|
| | Domain Name | First IP Address | Second IP Address |
| 1 | DomainName.com | 10.8.21.4 | 10.13.2.95 |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

2. In the 'Domain Name' field, enter the host name to be translated. You can enter a string up to 31 characters long.
3. In the 'First IP Address' field, enter the first IP address (in dotted format notation) that the hostname is translated to.
4. In the 'Second IP Address' field, enter the second IP address that the hostname is translated to.
5. Repeat steps 2 to 4, for each Internal DNS Table entry.
6. Click the **Submit** button to save your changes.
7. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

5.5.4.5 Internal SRV Table

The **Internal SRV Table** option (i.e., 'Internal SRV Table' screen) is used for resolving host names to DNS A-Records. Three different A-Records can be assigned to a hostname. Each A-Record contains the host name, priority, weight, and port.

You can also configure the Internal SRV table using the *ini* file parameter SRV2IP (refer to 'Networking Parameters' on page 299).



Note: If the Internal SRV table is configured, the gateway first tries to resolve a domain name using this table. If the domain name isn't found, the gateway performs an SRV resolution using an external DNS server.

➤ **To configure the Internal SRV table, take these 9 steps:**

1. Open the 'Internal SRV Table' screen (**Protocol Management** menu > **Routing Tables** submenu > **Internal SRV Table** option).

Figure 5-25: Internal SRV Table Screen

| Internal SRV Table | | | | | | | | | | | | | | |
|--------------------|-------------|----------------|------------|----------|--------|------|------------|----------|--------|------|------------|----------|--------|------|
| | Domain Name | Transport Type | DNS Name 1 | Priority | Weight | Port | DNS Name 2 | Priority | Weight | Port | DNS Name 3 | Priority | Weight | Port |
| 1 | | ▼ | | | | | | | | | | | | |
| 2 | | ▼ | | | | | | | | | | | | |
| 3 | | ▼ | | | | | | | | | | | | |
| 4 | | ▼ | | | | | | | | | | | | |
| 5 | | ▼ | | | | | | | | | | | | |
| 6 | | ▼ | | | | | | | | | | | | |
| 7 | | ▼ | | | | | | | | | | | | |
| 8 | | ▼ | | | | | | | | | | | | |
| 9 | | ▼ | | | | | | | | | | | | |
| 10 | | ▼ | | | | | | | | | | | | |

2. In the 'Domain Name' field, enter the hostname to be translated. You can enter a string up to 31 characters long.
3. From the 'Transport Type' drop-down list, select a transport type.
4. In the 'DNS Name 1' field, enter the first DNS A-Record to which the hostname is translated.
5. In the 'Priority', 'Weight' and 'Port' fields, enter the relevant values
6. Repeat steps 4 through 5, for the second and third DNS names, if required.
7. Repeat steps 2 through 6, for each Internal SRV Table entry.
8. Click the **Submit** button to save your changes.
9. To save the changes so they are available after a hardware reset or power fail, refer to 'Saving Configuration' on page 278.

5.5.4.6 Reasons for Alternative Routing

The 'Reasons for Alternative Routing' screen includes two groups: IP to Tel Reasons and Tel to IP Reasons. Each group enables you to define up to four different release reasons. If a call is released as a result of one of these reasons, the gateway tries to find an alternative route to that call. The release reason for IP-to-Tel calls is provided in Q.931 notation. The release reason for Tel→IP calls is provided in SIP 4xx, 5xx, and 6xx response codes. For Tel-to-IP calls an alternative IP address is provided; for IP-to-Tel calls an alternative hunt (analog modules) or trunk (digital modules) group is provided. Refer to 'Tel to IP Routing Table' on page 134 for information on defining an alternative IP address; refer to 'IP to Trunk Group Routing' on page 138 for information on defining an alternative trunk group.

You can use the 'Reasons for Alternative Routing' screen in the following example scenarios:

- For Tel-to-IP calls: when there is no response to an INVITE message (after INVITE retransmissions), and the gateway then issues an internal 408 'No Response' implicit release reason.
- For IP-to-Tel calls: when the destination is busy, and release reason #17 is issued or for other call releases that issue the default release reason (#3). Refer to DefaultReleaseCause in 'General Parameters' on page 103.



Note: The reasons for alternative routing option for Tel→IP calls only apply when a Proxy isn't used.

For configuring this table, you can also use the *ini* file parameters AltRouteCauseTel2IP and AltRouteCauseIP2Tel (refer to 'Number Manipulation and Routing Parameters' on page 359).

➤ **To configure the reasons for alternative routing, take these 5 steps:**

1. Open the 'Reasons for Alternative Routing' screen (**Protocol Management** menu > **Routing Tables** submenu > **Reasons for Alternative Routing** option).

Figure 5-26: Reasons for Alternative Routing Screen

| Reasons for Alternative Routing | | |
|---------------------------------|-----|---|
| IP to Tel Reasons | | |
| Reason 1 | 3 | ▼ |
| Reason 2 | 17 | ▼ |
| Reason 3 | 6 | ▼ |
| Reason 4 | 1 | ▼ |
| Tel to IP Reasons | | |
| Reason 1 | 408 | ▼ |
| Reason 2 | 486 | ▼ |
| Reason 3 | | ▼ |
| Reason 4 | | ▼ |

2. In the 'IP to Tel Reasons' group, select up to four different call failure reasons that invoke an alternative IP-to-Tel routing.
3. In the 'Tel to IP Reasons' group, select up to four different call failure reasons that invoke an alternative Tel-to-IP routing.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

5.5.4.7 Release Cause Mapping

The 'Release Cause Mapping' screen consists of two tables that allow the gateway to map up to 12 different SIP Responses to Q.850 Release Causes and vice versa, thereby overriding the hard-coded mapping mechanism (described in 'Release Cause Mapping' on page 144).

➤ **To configure the release cause mapping, take these 5 steps:**

1. Open the 'Release Cause Mapping' screen (**Protocol Management** menu > **Routing Tables** submenu > **Release Cause Mapping** option).

Figure 5-27: Release Cause Mapping Screen (e.g., ISDN to SIP)

| Release Cause Mapping from ISDN to SIP | | | |
|--|-------------|--|--------------|
| | Q.850 Cause | | SIP Response |
| 1 | 3 | | 486 |
| 2 | 18 | | 480 |
| 3 | 22 | | 403 |
| 4 | | | |
| 5 | | | |

2. In the 'Release Cause Mapping from ISDN to SIP' table, map (up to 12) different Q.850 Release Causes to SIP Responses.
3. In the 'Release Cause Mapping from SIP to ISDN' table, map (up to 12) different SIP Responses to Q.850 Release Causes.
4. Click the **Submit** button to save your changes.
5. To save the changes so they are available after a power fail, refer to 'Saving Configuration' on page 278.

5.5.5 Configuring the Profile Definitions

The Profiles feature provides the gateway with high-level adaptation when connected to a variety of equipment (from both Tel and IP sides) and protocols, each of which requires different system behavior. You can assign different Profiles (behavior) on a per call basis, using the Tel to IP and IP to Trunk Group Routing tables, or associate different Profiles to the gateway's endpoints (analog modules) or B-channels (digital modules). The Profiles contain parameters such as Coders, T.38 Relay, Voice and DTMF Gain, Silence Suppression, Echo Canceled, RTP DiffServ, Current Disconnect and more. The Profiles feature allows users to customize these parameters or turn them on or off, per source or destination routing and/or per the specific gateway trunks or ports (channels). For example, specific ports can be designated to have a profile which always uses G.711.

Each call can be associated with one or two Profiles: Tel Profile and/or IP Profile. If both IP and Tel profiles apply to the same call, the coders and other common parameters of the preferred Profile (determined by the Preference option) are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters take precedence and are applied.

Use the Profile Definitions submenu to configure profiles:

- **Coder Group Settings** (refer to 'Coder Group Settings' on page 145)
- **Tel Profile Settings** (refer to 'Tel Profile Settings' on page 146)
- **IP Profile Settings** (refer to 'IP Profile Settings' on page 148)



Note: The default values of the parameters in the Tel and IP Profiles are identical to the Embedded Web Server/*ini* file parameter values. If a value of a parameter is changed in the Embedded Web Server/*ini* file, it is automatically updated in the Profiles correspondingly. After any parameter in the Profile is modified by the user, modifications to parameters in the Embedded Web Server/*ini* file no longer impact that Profile.

5.5.5.1 Coder Group Settings

The **Coder Group Settings** option is used to define up to four different coder groups. These coder groups are used in the 'Tel Profile Settings' and 'IP Profile Settings' screens to assign different coders to Profiles.

For each coder group you can define up to five coders, where the first coder (and its attributes) in the list takes precedence over the second coder, and so on. The first coder is the highest priority coder and is used by the gateway whenever possible. If the far end gateway cannot use the coder assigned as the first coder, the gateway attempts to use the next coder and so forth. For a list of coders supported by the gateway, refer to 'Coders' on page 94.

You can also configure the coder groups using the *ini* file parameter *CoderName* (refer to 'SIP Configuration' on page 323Parameters).

➤ To configure coder groups, take these 11 steps:

1. Open the 'Coder Group Settings' screen (**Protocol Management** menu > **Profile Definitions** submenu > **Coder Group Settings** option).

Figure 5-28: Coder Group Settings Screen

| Coder Group Settings | | | | | | | | |
|----------------------|---|--------------------|---|------|---|--------------|---------------------|---|
| Coder Group ID | | | | | 1 | ▼ | | |
| Coder Name | ▼ | Packetization Time | ▼ | Rate | ▼ | Payload Type | Silence Suppression | ▼ |
| G.711A-law | ▼ | 10 | ▼ | 64 | ▼ | 8 | Disabled | ▼ |
| G.726 | ▼ | 20 | ▼ | 32 | ▼ | 2 | Disabled | ▼ |
| | ▼ | | ▼ | | ▼ | | | ▼ |
| | ▼ | | ▼ | | ▼ | | | ▼ |
| | ▼ | | ▼ | | ▼ | | | ▼ |

2. From the 'Coder Group ID' drop-down list, select a coder group ID that you want to add (up to four coder groups can be configured).
3. From the 'Coder Name' drop-down list, select the first coder for the coder group. For a full list of available coders and their corresponding attributes, refer to 'Coders' on page 94.
4. From the 'Packetization Time' drop-down list, select the packetization time (in msec) for the coder. The packetization time determines how many coder payloads are combined into a single RTP packet.
5. From the 'Rate' drop-down list, select the bit rate (in kbps) for the coder you selected.
6. In the 'Payload Type' field, if the payload type for the coder you selected is dynamic, enter a value from 0 to 120 (payload types of 'well-known' coders cannot be modified). The payload type identifies the format of the RTP payload.
7. From the 'Silence Suppression' drop-down list, enable or disable the silence suppression option for the coder you selected.
8. Repeat steps 3 through 7 for the second to fifth coders (optional).
9. Repeat steps 2 through 8 for the second to fourth coder groups (optional).
10. Click the **Submit** button to save your changes.
11. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.


Notes:

- Each coder can appear only once.
- The ptime specifies the packetization time the gateway expects to receive. The gateway always uses the ptime requested by the remote side for sending RTP packets. If not specified, the packetization time (ptime) gets a default value.
- Only the ptime of the first coder in the defined coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined.
- For G.729 it is also possible to select silence suppression without adaptations.
- If the coder G.729 is selected and silence suppression is enabled (for this coder), the gateway includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception to this logic is when the remote gateway is a Cisco device (IsCiscoSCEMode).

5.5.5.2 Tel Profile Settings

The **Tel Profile Settings** option is used to define up to nine different Tel Profiles. These Profiles are used in the 'Trunk Group Table' screen where they can be assigned to the gateway's channels, thereby applying different behaviors to different channels.

You can also configure Tel Profiles using the *ini* file parameter TelProfile (refer to 'SIP Configuration Parameters' on page 323).

➤ **To configure Tel Profiles, take these 9 steps:**

1. Open the 'Tel Profile Settings' screen (**Protocol Management** menu > **Profile Definitions** submenu > **Tel Profile Settings** option).

| Tel Profile Settings | |
|--|---------------------|
| Profile ID | 1 |
| Profile Name | |
| Profile Parameters | |
| Profile Preference | 1 |
| Fax Signaling Method | No Fax |
| Dynamic Jitter Buffer Minimum Delay [msec] | 10 |
| Dynamic Jitter Buffer Optimization Factor | 10 |
| RTP IP Diff Serv | 46 |
| Signaling DiffServ | 50 |
| Voice Volume (-32 to 31 dB) | 0 |
| DTMF Volume (-31 to 0 dB) | -11 |
| Input Gain (-32 to 31 dB) | 0 |
| Enable Digit Delivery | Disable |
| Enable Polarity Reversal | Disable |
| Enable Current Disconnect | Disable |
| Enable Digit Delivery | Disable |
| MWI Analog Lamp | Disable |
| MWI Display | Disable |
| Echo Canceler | Enable |
| Max. Hook-Flash Detection Period [msec] | 700 |
| Enable Early Media | Disable |
| Progress Indicator to IP | Not Configured |
| Time For Reorder Tone [sec] | 255 |
| Coder Group | |
| Coder Group | Default Coder Group |

2. From the 'Profile ID' drop-down list, select the Tel Profile identification number you want to edit (up to four Tel Profiles can be configured).
3. In the 'Profile Name' field, enter an arbitrary name that enables you to identify the Profile intuitively and easily.

4. From the 'Profile Preference' drop-down list, select the preference (1-20) of the current Profile. The preference option is used to determine the priority of the Profile. Where '20' is the highest preference value. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk in the description of the parameter TelProfile) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
Note: If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used). The order of the coders is determined by the preference.
5. Configure the Profile's parameters according to your requirements. For detailed information on each parameter, refer to the description of the screen in which it is configured as an individual parameter.
6. From the 'Coder Group' drop-down list, select the coder group to which you want to assign the Profile. You can select the gateway's default coders (refer to 'Coders' on page 94) or one of the coder groups you defined in the 'Coder Group Settings' screen (refer to 'Coder Group Settings' on page 145).
7. Repeat steps 2 to 6 for the second to fifth Tel Profiles (optional).
8. Click the **Submit** button to save your changes.
9. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

5.5.5.3 IP Profile Settings

The **IP Profile Settings** option is used to define up to four different IP Profiles. These Profiles are used in the 'Tel to IP Routing' and 'IP to Trunk Group Routing Table' screens for associating IP Profiles to routing rules. IP Profiles can also be used when working with Proxy server (set AlwaysUseRouteTable to 1).

You can also configure the IP Profiles using the *ini* file parameter IPProfile (refer to 'SIP Configuration Parameters' on page 323).

➤ **To configure the IP Profile settings, take these 9 steps:**

1. Open the 'IP Profile Settings' screen (**Protocol Management** menu > **Profile Definitions** submenu > **IP Profile Settings** option).

Figure 5-29: IP Profile Settings Screen

| IP Profile Settings | |
|--|---------------------|
| Profile ID | 1 |
| Profile Name | |
| Profile Parameters | |
| Profile Preference | 1 |
| Fax Signaling Method | No Fax |
| Dynamic Jitter Buffer Minimum Delay [msec] | 70 |
| Dynamic Jitter Buffer Optimization Factor | 10 |
| RTP IP Diff Serv | 46 |
| Signaling DiffServ | 40 |
| RTP Redundancy Depth | 0 |
| Remote RTP Base UDP Port | 0 |
| CNG Detector Mode | Disable |
| Modems Transport Type | Enable Bypass |
| NSE Mode | Disable |
| Play Ringback Tone to IP | Don't Play |
| Enable Early Media | Disable |
| Progress Indicator to IP | Not Configured |
| Echo Cancellor | Enable |
| Coder Group | |
| Coder Group | Default Coder Group |

2. From the 'Profile ID' drop-down list, select the IP Profile you want to edit (up to four IP Profiles can be configured).
3. In the 'Profile Name' field, enter an arbitrary name that enables you to identify the Profile intuitively and easily.

4. From the 'Profile Preference' drop-down list, select the preference (1-20) of the current Profile. The preference option is used to determine the priority of the Profile. Where '20' is the highest preference value. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk in the description of the parameter IPProfile) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
Note: If the coder lists of both IP and Tel Profiles apply to the same call, an intersection of the coders is performed (i.e., only common coders remain). The order of the coders is determined by the preference.
5. Configure the Profile's parameters according to your requirements. For detailed information on each parameter, refer to the description of the screen in which it is configured as an individual parameter.
6. From the 'Coder Group' drop-down list, select the coder group you want to assign to the Profile. You can select the gateway's default coders (refer to 'Coders' on page 94) or one of the coder groups you defined in the Coder Group Settings screen (refer to 'Coder Group Settings' on page 145).
7. Repeat steps 2 to 6 for the second to fifth IP Profiles (optional).
8. Click the **Submit** button to save your changes.
9. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

5.5.6 Configuring the Trunk Group Table

The **Trunk Group Table** option is used to assign trunk groups, profiles, and logical telephone numbers to the gateway's channels. Trunk Groups are used for routing IP-to-Tel calls with common rules. Channels that are not defined are disabled.

You can also use the *ini* file parameter TrunkGroup_x to configure the Trunk Groups (refer to 'Number Manipulation and Routing Parameters' on page 359).

➤ To configure the Trunk Group table, take these 4 steps:

1. Open the 'Trunk Group Table' screen (**Protocol Management** menu > **Trunk Group**).

| Trunk Group Table | | | | | | | | |
|-------------------|--------------------|------------|----------|----------|--------------|----------------|------------|--|
| Trunk Group Index | | | | | | 1-12 ▾ | | |
| Group Index | Module | From Trunk | To Trunk | Channels | Phone Number | Trunk Group ID | Profile ID | |
| 1 | Module 1 Digital ▾ | 1 ▾ | 1 ▾ | 1-31 | | 1 | 0 | |
| 2 | ▾ | ▾ | ▾ | | | | | |
| 3 | ▾ | ▾ | ▾ | | | | | |
| 4 | ▾ | ▾ | ▾ | | | | | |

2. Configure the Trunk Group according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to the flash memory, refer to 'Saving Configuration' on page 278.

Table 5-24: Trunk Group Table

| Parameter | Description |
|-----------------------|--|
| Module | <p>The module for which you want to define the trunk group. Valid options include:</p> <ul style="list-style-type: none"> Module 1 Digital Module 2 FXO Module 3 FXS |
| From Trunk | <p>Starting physical trunk number (). Note: Applicable only to digital modules.</p> |
| To Trunk | <p>Ending physical trunk number ().</p> |
| Channels | <p>Represents the channels or ports on the gateway (analog module), or trunk's B-channels (digital module). To enable the trunk's channels, enter the channels number in this field. [n-m] represents a range of channels. For example, [1-24] specifies channels 1 through 24. Notes:</p> <ul style="list-style-type: none"> The number of defined channels must not exceed the number of the trunk's B-channels (1 - 24 for T1 spans; 1 - 31 for E1 spans). To represent all channels, enter a single asterisk (*). |
| Phone Number | <p>Enter the first number in an ordered sequence that is assigned to the range of corresponding channels defined in the adjacent 'Channels' field. Note: This field is optional. The logical numbers defined in this field are used when an incoming PSTN / PBX call doesn't contain the calling number or called number (the latter being determined by the parameter ReplaceEmptyDstWithPortNumber); these numbers are used to replace them. These logical numbers are also used for channel allocation for IP-to-Tel calls if the trunk group's 'Channel Select Mode' is set to 'By Dest Phone Number'.</p> |
| Trunk Group ID | <p>The trunk group ID (1-99) assigned to the corresponding channels. The same trunk group ID can be used for more than one group of channels. Trunk group ID is used to define a group of common behavior channels that are used for routing IP-to-Tel calls. If an IP-to-Tel call is assigned to a trunk group, the call is routed to the channel or channels that correspond to the trunk group ID. You can configure the 'Trunk Group Settings table' to determine the method in which new calls are assigned to channels within the trunk groups (refer to 'Configuring the Trunk Group Settings' on page 152). Note: You must configure the 'IP to Trunk Group Routing Table' screen (assigns incoming IP calls to the appropriate trunk group). If you do not configure the IP to Trunk Group Routing Table, calls do not complete. For information on how to configure this table, refer to 'IP to Trunk Group Routing' on page 138.</p> |
| Profile ID | <p>The Tel profile ID that is assigned to the B-channels defined in the 'Channels' field.</p> |

5.5.7 Configuring the Trunk Group Settings

The **Trunk Group Settings** option is used to determine the method in which new calls are assigned to channels within each trunk group. If such a rule doesn't exist (for a specific Trunk group), the global rule, defined by the 'Channel Select Mode' parameter (**Protocol Definition > General Parameters**), applies.

You can also configure the Trunk Group Settings table using the *ini* file parameter TrunkGroupSettings (refer to 'Number Manipulation and Routing Parameters' on page 359).

➤ **To configure the Trunk Group Settings table, take these 5 steps:**

1. Open the 'Trunk Group Settings' screen (**Protocol Management** menu > **Trunk Group Settings**).

Figure 5-30: Trunk Group Settings Screen

| Trunk Group Settings | | | |
|----------------------|---------------------|--------------------|---------------|
| Routing Index | | 1-12 ▼ | |
| Trunk Group ID | Channel Select Mode | Registration Mode | |
| 1 | 1 | Cyclic Ascending ▼ | Per Gateway ▼ |
| 2 | 2 | Ascending ▼ | Per Gateway ▼ |
| 3 | 3 | Descending ▼ | Per Gateway ▼ |
| 4 | | ▼ | ▼ |
| 5 | | ▼ | ▼ |
| 6 | | ▼ | ▼ |
| 7 | | ▼ | ▼ |
| 8 | | ▼ | ▼ |
| 9 | | ▼ | ▼ |
| 10 | | ▼ | ▼ |
| 11 | | ▼ | ▼ |
| 12 | | ▼ | ▼ |

2. From the 'Routing Index' drop-down list, select the range of entries that you want to edit (up to 24 entries can be configured).
3. Configure the Trunk Group Settings table according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-25: Hunt Group Settings Parameters

| Mode | Description |
|----------------------------|---|
| Trunk Group ID | Trunk Group ID to which you want to determine the method in which new calls are assigned to channels within the trunk group. |
| Channel Select Mode | <p>Method in which new calls are assigned to channels within the Trunk Group entered in the 'Trunk Group ID' field:</p> <ul style="list-style-type: none"> By Dest Phone Number = Selects the gateway port according to the called number (refer to the note below). Cyclic Ascending = Selects the next available channel in an ascending cycle order. Always select the next higher channel number in the Trunk Group. When the gateway reaches the highest channel number in the Trunk Group, it selects the lowest channel number in the Trunk Group and then starts ascending again (default). Ascending = Selects the lowest available channel. It always starts at the lowest channel number in the Trunk Group and if that channel is not available, it selects the next higher channel. Cyclic Descending = Selects the next available channel in descending cycle order. It always selects the next lower channel number in the Trunk Group. When the gateway reaches the lowest channel number in the Trunk Group, it selects the highest channel number in the Trunk Group and then start descending again. Descending = Selects the highest available channel. It always starts at the highest channel number in the Trunk Group and if that channel is not available, selects the next lower channel. Dest Number + Cyclic Ascending = It first selects the gateway port according to the called number (refer to the note below). If the called number isn't found, then it selects the next available channel in ascending cyclic order. Note that if the called number is found, but the port associated with this number is busy, the call is released. By Source Phone Number = Selects the gateway port according to the calling number. Trunk Cyclic Ascending = Selects the gateway port from the first channel of the next trunk (next to the trunk from which the previous channel was allocated). Note: Not applicable for analog interfaces. |
| Registration Mode | <p>Registration mode for the Trunk Group:</p> <ul style="list-style-type: none"> Per Endpoint = separate registration for each channel in the Trunk Group. Per Gateway = single registration for the whole Trunk Group (default). Don't Register |



Note: The internal numbers of the gateway's channels are defined in the 'Trunk Group Table' under the 'Phone Number' column. For detailed information on the 'Trunk Group Table', refer to 'Configuring the Trunk Group Table' on page 150).

5.5.8 Configuring the Endpoint Settings

The **Endpoint Settings** submenu enables you to configure port-specific parameters.



Note: The Endpoint Settings menu is only applicable to the analog modules.

5.5.8.1 Authentication

The 'Authentication' screen (typically used for FXS modules) defines a username and password combination for authenticating each gateway port.

The 'Authentication Mode' parameter (described in 'Proxy & Registration Parameters' on page 84) determines whether authentication is performed per port or for the entire gateway. If authentication is performed for the entire gateway, this table is ignored.

You can also configure Authentication using the *ini* file parameter table Authentication (refer to 'SIP Configuration Parameters' on page 323).



Note: If either the username or password field is omitted, the port's phone number (defined in Configuring the Trunk Group Table on page 150) and global password (refer to the parameter 'Password' described in 'Proxy & Registration Parameters' on page 84) are used instead.

➤ To configure the Authentication Table, take these 6 steps:

1. Set the 'Authentication Mode' parameter to 'Per Endpoint' (refer to 'Proxy & Registration Parameters' on page 84).
2. Open the 'Authentication' screen (**Protocol Management** menu > **Endpoint Settings** > **Authentication** option).

Figure 5-31: Authentication Screen

| Authentication | | |
|---------------------|----------------------|----------------------|
| Gateway Port | User Name | Password |
| Module 2 Port 1 FXO | <input type="text"/> | <input type="text"/> |
| Module 2 Port 2 FXO | <input type="text"/> | <input type="text"/> |
| Module 2 Port 3 FXO | <input type="text"/> | <input type="text"/> |
| Module 2 Port 4 FXO | <input type="text"/> | <input type="text"/> |
| Module 3 Port 1 FXS | <input type="text"/> | <input type="text"/> |
| Module 3 Port 2 FXS | <input type="text"/> | <input type="text"/> |
| Module 3 Port 3 FXS | <input type="text"/> | <input type="text"/> |
| Module 3 Port 4 FXS | <input type="text"/> | <input type="text"/> |

3. In the 'User Name' and 'Password' fields for a port, enter the username and password combination respectively.
4. Repeat Step 3 for each port.
5. Click the **Submit** button to save your changes.
6. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

5.5.8.2 Automatic Dialing

The 'Automatic Dialing' screen is used to define telephone numbers that are automatically dialed when a specific port is used.

You can also configure automatic dialing using the *ini* file parameter TargetOfChannel (refer to 'Analog Telephony Parameters' on page 350).

➤ **To configure Automatic Dialing take these 6 steps:**

1. Open the 'Automatic Dialing' screen (**Protocol Management** menu > **Endpoint Settings** submenu > **Automatic Dialing** option).

| Automatic Dialing | | |
|---------------------|--------------------------|---|
| Gateway Port | Destination Phone Number | Auto Dial Status |
| Module 2 Port 1 FXO | 200 | Enable <input type="button" value="v"/> |
| Module 2 Port 2 FXO | 201 | Enable <input type="button" value="v"/> |
| Module 2 Port 3 FXO | 202 | Enable <input type="button" value="v"/> |
| Module 2 Port 4 FXO | 203 | Enable <input type="button" value="v"/> |
| Module 3 Port 1 FXS | 204 | Enable <input type="button" value="v"/> |
| Module 3 Port 2 FXS | 205 | Enable <input type="button" value="v"/> |
| Module 3 Port 3 FXS | 206 | Enable <input type="button" value="v"/> |
| Module 3 Port 4 FXS | 207 | Enable <input type="button" value="v"/> |

2. In the 'Destination Phone Number' field corresponding to a port, enter the telephone number to dial.
3. In the 'Auto Dial Status' field, select one of the following:
 - Enable **[1]**: When making a call, the number in the 'Destination Phone Number' field is automatically dialed if the phone is offhooked (for FXS modules) or ring signal is applied to a port (FXO modules).
 - Disable **[0]**: The automatic dialing option on the specific port is disabled (the number in the 'Destination Phone Number' field is ignored).
 - Hotline **[2]**: When a phone is offhooked and no digit is dialed for HotLineToneDuration, the number in the 'Destination Phone Number' field is automatically dialed (applies to FXS and FXO modules).
4. Repeat step 3 for each port you want to use for Automatic Dialing.

5. Click the **Submit** button to save your changes.
6. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.


Notes:

- After a ring signal is detected on an 'Enabled' FXO port, the gateway initiates a call to the destination number without seizing the line. The line is seized only after the call is answered.
- After a ring signal is detected on a 'Disabled' or 'Hotline' FXO port, the gateway seizes the line.

5.5.8.3 Caller ID

The 'Caller Display Information' screen is used to send (to IP) Caller ID information when a call is made using the gateway (relevant to both FXS and FXO). The person receiving the call can use this information for caller identification. The information in this screen (table) is sent in an INVITE message in the 'From' header. For information on Caller ID restriction according to destination / source prefixes, refer to 'Configuring the Number Manipulation Tables' on page 125.

You can also configure the Caller Display Information table using the *ini* file parameter CallerDisplayInfo (refer to 'Analog Telephony Parameters' on page 350).



Note: If Caller ID name is detected on an FXO line (EnableCallerID = 1), it is used instead of the Caller ID name defined in this table (FXO modules only).

➤ **To configure the Caller Display Information, take these 6 steps:**

1. Open the 'Caller Display Information' screen (**Protocol Management** menu > **Endpoint Settings** submenu > **Caller ID** option).

| Caller Display Information | | | | |
|----------------------------|--------|-----|----------------|--------------|
| Gateway Port | | | Caller ID/Name | Presentation |
| Module 2 | Port 1 | FXO | Private | Restricted |
| Module 2 | Port 2 | FXO | | Allowed |
| Module 2 | Port 3 | FXO | | Allowed |
| Module 2 | Port 4 | FXO | | Allowed |
| Module 3 | Port 1 | FXS | Susan C. | Allowed |
| Module 3 | Port 2 | FXS | Lee D. | Restricted |
| Module 3 | Port 3 | FXS | Mark M. | Restricted |
| Module 3 | Port 4 | FXS | John H. | Allowed |

2. In the 'Caller ID/Name' field, enter the Caller ID string. The Caller ID string can contain up to 18 characters. Note that when the FXS modules receives 'Private' or 'Anonymous' strings in the From header, it doesn't send the calling name or number to the Caller ID display.
3. In the 'Presentation' field, select 'Allowed' **[0]** to send the string defined in the 'Caller ID/Name' field when a Tel-to-IP call is made using this gateway port. Select 'Restricted' **[1]** if you don't want to send this string. (Refer to the note below.)
4. Repeat steps 2 and 3 for each gateway port.
5. Click the **Submit** button to save your changes.
6. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

**Notes:**

- When the 'Presentation' field is set to 'Restricted', the caller identity is passed to the remote side using only the P-Asserted-Identity and P-Preferred-Identity headers (AssertedIdMode).
- The value of the 'Presentation' field can (optionally) be overridden by configuring the 'Presentation' parameter in the 'Source Number Manipulation' table.
-

5.5.8.4 Call Forward

The gateway allows you to forward incoming IP→Tel calls (using 302 response) based on the gateway port to which the call is routed (applicable only to FXS modules).

The 'Call Forwarding Table' screen is applicable only if the Call Forward feature is enabled. To enable Call Forward, set 'Enable Call Forward' to 'Enable' in the 'Supplementary Services' screen, or EnableForward = 1 in the *ini* file (refer to 'SIP Configuration Parameters' on page 323).

You can also configure the Call Forward table using the *ini* file parameter FwdInfo (refer to 'Analog Telephony Parameters' on page 350).

➤ **To configure the Call Forward table, take these 4 steps:**

1. Open the 'Call Forward Table' screen (**Protocol Management** menu > **Endpoint Settings** submenu > **Call Forward** option).

| Call Forward Table | | | | | | |
|--------------------|--------|-----|--|----------------|-------------------------|---------------------------|
| Gateway Port | | | | Forward Type | Forward to Phone Number | Time for No Reply Forward |
| Module 2 | Port 1 | FXO | | No Answer | 203 | 30 |
| Module 2 | Port 2 | FXO | | Deactivate | | |
| Module 2 | Port 3 | FXO | | Deactivate | | |
| Module 2 | Port 4 | FXO | | Deactivate | | |
| Module 3 | Port 1 | FXS | | On busy | 201 | |
| Module 3 | Port 2 | FXS | | Unconditional | 202@10.2.1.1 | |
| Module 3 | Port 3 | FXS | | Do Not Disturb | 203 | |
| Module 3 | Port 4 | FXS | | Deactivate | | |

2. Configure the Call Forward parameters for each port according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-26: Call Forward Table

| Parameter | Description |
|----------------------------------|--|
| Forward Type | <ul style="list-style-type: none"> ▪ [0] Deactivate = Don't forward incoming calls (default). ▪ [1] On Busy = Forward incoming calls when the gateway port is busy. ▪ [2] Unconditional = Forward any incoming call to the phone number specified in the 'Forward to Phone Number' field. ▪ [3] No Answer = Forward incoming calls that are not answered within the time specified in the 'Time for No Reply Forward' field. ▪ [4] On Busy or No Answer = Forward incoming calls when the port is busy or when calls are not answered after a configurable period of time. ▪ [5] Do Not Disturb = Immediately reject incoming calls. |
| Forward to Phone Number | Enter the telephone number or URI (number@IP address) to which the call is forwarded. Note: If this field only contains a telephone number and a Proxy isn't used, the 'forward to' phone number must be specified in the 'Tel to IP Routing' table of the forwarding gateway. |
| Time for No Reply Forward | If you have set the Forward Type for this port to No Answer, enter the number of seconds the gateway waits before forwarding the call to the phone number specified. |

5.5.8.5 Caller ID Permissions

The 'Caller ID Permissions' screen is used to enable or disable (per port) the Caller ID generation (for FXS modules) and detection (for FXO modules). If a port isn't configured, its Caller ID generation / detection are determined according to the global parameter EnableCallerID (described in 'Supplementary Services' on page 113).

You can also configure the Caller ID Permissions table using the *ini* file parameter EnableCallerID (refer to 'Analog Telephony Parameters' on page 350).

➤ **To configure the Caller ID Permissions Table, take these 5 steps:**

1. Open the 'Caller ID Permissions' screen (**Protocol Management** menu > **Endpoint Settings** > **Caller ID Permissions** option).

| Caller ID Permissions | | | | |
|-----------------------|--------|-----|--|-----------|
| Gateway Port | | | | Caller ID |
| Module 2 | Port 1 | FXO | | Disable |
| Module 2 | Port 2 | FXO | | Disable |
| Module 2 | Port 3 | FXO | | Disable |
| Module 2 | Port 4 | FXO | | |
| Module 3 | Port 1 | FXS | | Enable |
| Module 3 | Port 2 | FXS | | |
| Module 3 | Port 3 | FXS | | |
| Module 3 | Port 4 | FXS | | |

2. In the 'Caller ID' field, select one of the following:
 - Enable: Enables Caller ID generation (FXS) or detection (FXO) for the specific port.
 - Disable: Caller ID generation (FXS) or detection (FXO) for the specific port is disabled.
 - Empty: Caller ID generation (FXS) or detection (FXO) for the specific port is determined according to the parameter EnableCallerID (described in 'Supplementary Services' on page 113).
3. Repeat Step 2 for each port.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

5.5.8.6 Call Waiting

The 'Call Waiting' screen is used to configure call waiting per gateway port.

You can also configure the Call Waiting table using the *ini* file parameter `CallWaitingPerPort` (refer to 'SIP Configuration Parameters' on page 323).



Note: If Call Waiting per port is not configured (using the 'Call Waiting' screen, then use the global (i.e., for all ports) call waiting parameter 'Enable Call Waiting' (`EnableCallWaiting`) in 'Supplementary Services' on page 113).

➤ **To configure Call Waiting, take these 5 steps:**

1. Open the 'Call Waiting' screen (**Protocol Management** menu > **Endpoint Settings** > **Call Waiting** option).

| Call Waiting | | | |
|--------------|------------|----------------------------|---|
| Gateway Port | | Call Waiting Configuration | |
| Module 2 | Port 1 FXO | Enable | ▼ |
| Module 2 | Port 2 FXO | | ▼ |
| Module 2 | Port 3 FXO | | ▼ |
| Module 2 | Port 4 FXO | | ▼ |
| Module 3 | Port 1 FXS | | ▼ |
| Module 3 | Port 2 FXS | | ▼ |
| Module 3 | Port 3 FXS | | ▼ |
| Module 3 | Port 4 FXS | | ▼ |

2. For each relevant, from the 'Call Waiting Configuration'; drop-down list, select one of the following:
 - 'Enable': Enables call waiting for the specific port. when an FXS gateway module receives a call on a busy endpoint, it responds with a 182 response (and not with a 486 busy). The gateway plays a call waiting indication signal. When hook-flash is detected, the gateway switches to the waiting call. The gateway that initiated the waiting call plays a Call Waiting Ringback tone to the calling party after a 182 response is received.
 - 'Disable': No call waiting for the specific port.
 - Empty: Call waiting is determined according to the global (i.e., for all ports) parameter `EnableCallWaiting` (described in 'Supplementary Services' on page 113).
3. Repeat Step 2 for each port.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

5.5.9 Configuring the Digital Gateway Parameters

The 'Digital Gateway' screen is used to configure miscellaneous digital parameters.

➤ **To configure the digital gateway parameters, take these 4 steps:**

1. Open the 'Digital gateway Parameters' screen (**Protocol Management** menu > **Digital Gateway Parameters**).

Figure 5-32: Digital Gateway Parameters Screen

| Digital Gateway Parameters | |
|---|----------------|
| B-channel Negotiation | Exclusive |
| Swap Redirect and Called Numbers | No |
| MFC R2 Category | 1 |
| Disconnect Call on Detection of Busy Tone | Yes |
| ! Enable TDM Tunneling | Disable |
| Send Screening Indicator to IP | Not Configured |
| Send Screening Indicator to ISDN | Not Configured |
| Add IE in SETUP | |
| Trunk Groups to Send IE | |
| Enable User-to-User IE for Tel to IP | Disable |
| Enable User-to-User IE for IP to Tel | Disable |
| Enable ISDN Tunneling Tel to IP | Disable |
| Enable QSIG Tunneling | Disable |
| Enable ISDN Tunneling IP to Tel | Disable |
| ISDN Transfer on Connect | Alert |
| Remove CLI when Restricted | No |
| Default Cause Mapping From ISDN to SIP | 0 |
| Add Prefix to Redirect Number | |
| Enable Calling Party Category | Disable |
| MLPP | |
| Call Priority Mode | Disable |
| MLPP Default Namespace | DSN |
| Default Call Priority | 0 |
| MLPP Diffserv | 50 |

2. Configure the Digital Gateway parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-27: Digital Gateway Parameters

| Parameter | Description |
|--|---|
| B-channel Negotiation [BchannelNegotiation] | <p>Determines the ISDN B-Channel negotiation mode.</p> <ul style="list-style-type: none"> [0] Preferred = Preferred [1] Exclusive = Exclusive (default) [2] Any = Any <p>Notes:</p> <ul style="list-style-type: none"> Applicable to ISDN protocols. The Any option is only applicable if TerminationSide = 0 (User side). |
| Swap Redirect and Called Numbers [SwapRedirectNumber] | <ul style="list-style-type: none"> [0] No = Don't change numbers (default) [1] Yes = Incoming ISDN call that includes redirect number (sometimes referred as 'original called number') uses this number instead of the called number. |
| MFC R2 Category [R2Category] | <p>MFC R2 Calling Party Category (CPC). The parameter provides information on calling party such as National or International call, Operator or Subscriber and Subscriber priority. The parameter range is 1 to 15, defining one of the MFC R2 tones.</p> |
| Disconnect Call on Detection of Busy Tone [DisconnectOnBusyTone] | <ul style="list-style-type: none"> [0] No = Do not disconnect call on detection of busy tone. [1] Yes = Disconnect call on detection of busy tone (default). <p>Note: This parameter is applicable to CAS and ISDN protocols.</p> |
| Enable TDM Tunneling [EnableTDMoverIP] | <ul style="list-style-type: none"> [0] Disable = Disabled (default). [1] Enable = TDM Tunneling is enabled. <p>When TDM Tunneling is enabled, the originating gateway automatically initiates SIP calls from all enabled B-channels belonging to the E1/T1/J1 spans that are configured with the 'Transparent' protocol. The called number of each call is the internal phone number of the B-channel that the call originates from. The IP to Trunk Group routing table is used to define the destination IP address of the terminating gateway. The terminating gateway automatically answers these calls if its E1/T1 protocol is set to 'Transparent' (ProtocolType = 5).</p> |
| Send Screening Indicator to IP [ScreeningInd2IP] | <p>The parameter can overwrite the calling number screening indication for ISDN Tel-to-IP calls.</p> <ul style="list-style-type: none"> [-1] Not Configured = not configured (interworking from ISDN to IP) or set to 0 for CAS. [0] User Provided = user provided, not screened. [1] User Passed = user provided, verified and passed. [2] User Failed = user provided, verified and failed. [3] Network Provided = network provided. <p>Note: Applicable only if Remote Party ID (RPID) header is enabled.</p> |

Table 5-27: Digital Gateway Parameters

| Parameter | Description |
|--|---|
| Send Screening Indicator to ISDN [ScreeningInd2ISDN] | Overwrites the screening indicator of the calling number for IP→Tel (ISDN) calls. <ul style="list-style-type: none"> ▪ [-1] Not Configured = Not configured (interworking from IP to ISDN) (default). ▪ [0] User Provided = user provided, not screened. ▪ [1] User Passed = user provided, verified and passed. ▪ [2] User Failed = user provided, verified and failed. ▪ [3] Network Provided = network provided. |
| Add IE in SETUP [AddIEinSetup] | This parameter enables to add an optional Information Element data (in hex format) to ISDN SETUP message. For example: to add the following IE: '0x20,0x02,0x00,0xe1', define: 'AddIEinSetup = 200200e1'. Note: This IE is sent from the Trunk Group IDs defined by the parameter 'SendIEonTG'. |
| Trunk Groups to Send IE [SendIEonTG] | A list of Trunk Group IDs (up to 50 characters) from where the optional ISDN IE, defined by the parameter AddIEinSetup is sent. For example: 'SendIEonTG = 1,2,4,10,12,6'. |
| Enable User-to-User IE for Tel to IP [EnableUUITel2IP] | <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enable transfer of User-to-User Information Element (UUIE) from PRI to SIP. <p>The gateway supports the following interworking: SETUP to INVITE, CONNECT to 200 OK, and USER INFORMATION to INFO.</p> <p>Note: The interworking of User-to-User IE to SIP INFO is supported only on 4ESS PRI variant.</p> |
| Enable User-to-User IE for IP to Tel [EnableUUIP2Tel] | <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enable transfer of (UUIE) from SIP INVITE message to PRI Setup message. <p>The gateway supports the following interworking: INVITE to SETUP, 200 OK to CONNECT, and INFO to USER INFORMATION.</p> <p>Note: The interworking of User-to-User IE to SIP INFO is supported only on 4ESS PRI variant.</p> |

Table 5-27: Digital Gateway Parameters

| Parameter | Description |
|--|--|
| Enable ISDN Tunneling Tel to IP [EnableISDNTunnelingTel2IP] | <p>Valid options include:</p> <ul style="list-style-type: none"> [0] Disable = Disable (default). [1] Using Header = Enable ISDN Tunneling from ISDN PRI to SIP using a proprietary SIP header. [2] Using Body = Enable ISDN Tunneling from ISDN PRI to SIP using a dedicated message body. <p>When ISDN Tunneling is enabled, the gateway sends all ISDN PRI messages using the correlated SIP messages. Setup is tunneled using INVITE, all mid-call messages are tunneled using INFO, and Disconnect/Release is tunneled using BYE. The raw data from the ISDN is inserted into a proprietary SIP header (X-ISDNTunnelingInfo) or a dedicated message body (application/isdn) in the SIP messages.</p> <p>Note: It is necessary to set the parameter ISDNDuplicateQ931BuffMode to 128 (duplicate all messages) for this mechanism to function.</p> |
| Enable QSIG Tunneling [EnableQSIGTunneling] | <p>Enables QSIG tunneling over SIP according to <draft-elwell-sipping-qsig-tunnel-03>.</p> <ul style="list-style-type: none"> [0] Disable = Disable (default). [1] Enable = Enable QSIG tunneling from QSIG to SIP and vice versa. <p>When QSIG tunneling is enabled, all QSIG messages are sent as raw data in corresponding SIP messages using a dedicated message body. Note that QSIG tunneling must be enabled on both the originating and terminating gateways.</p> <p>Note: It is necessary to set the parameter ISDNDuplicateQ931BuffMode to 128 (duplicate all messages) so that this mechanism can function.</p> |
| Enable ISDN Tunneling IP to Tel [EnableISDNTunnelingIP2Tel] | <p>Valid options include:</p> <ul style="list-style-type: none"> [0] Disable = Disable (default). [1] Using Header = Enable ISDN Tunneling from SIP to ISDN PRI using a proprietary SIP header. [2] Using Body = Enable ISDN Tunneling from SIP to ISDN PRI using a dedicated message body. <p>When ISDN Tunneling is enabled, the gateway extracts raw data received in a proprietary SIP header (X-ISDNTunnelingInfo) or a dedicated message body (application/isdn) in the SIP messages and sends the data as ISDN messages to the PSTN side.</p> |

Table 5-27: Digital Gateway Parameters

| Parameter | Description |
|---|--|
| ISDN Transfer On Connect [SendISDNTransferOnConnect] | <ul style="list-style-type: none"> [0] Alert = Enable ISDN Transfer if outgoing call is in Alert state (default). [1] Connect = Enable ISDN Transfer only if outgoing call is in Connect state. <p>This parameter is used for the ECT/TBCT/RLT ISDN Transfer methods. Usually, the gateway requests the PBX to connect an incoming and an outgoing call. This parameter determines if the outgoing call (from the gateway to the PBX) must be connected before the transfer is initiated.</p> |
| Remove CLI when Restricted [RemoveCLIWhenRestricted] | <p>Determines (for IP to Tel calls) whether the Calling Number IE and Calling Name IE are removed from the outgoing ISDN Setup message if the presentation is set to Restricted.</p> <ul style="list-style-type: none"> [0] No = IE aren't removed (default). [1] Yes = IE are removed. |
| Default Cause Mapping From ISDN to SIP [DefaultCauseMapISDN2IP] | <p>Defines a single default ISDN Release Cause that is used (in ISDN to IP calls) instead of all received release causes except when the following Q.931 cause values are received: Normal Call Clearing (16), User Busy (17), No User Responding (18) or No Answer from User (19).</p> <p>The range is valid Q.931 release causes (0 to 127). The default value is 0 (indicates that the parameter is not configured - static mapping is used).</p> |
| Add Prefix to Redirect Number [Prefix2RedirectNumber] | <p>Defines a string Prefix that is added to the Redirect number received from the Tel side. This Prefix is added to the Redirect Number in the Diversion header.</p> <p>The valid range is an 8 character string. The default is an empty string.</p> |
| Enable Calling Party Category [EnableCallingPartyCategory] | <p>Determines whether Calling Party Category is relayed between SIP and PRI.</p> <ul style="list-style-type: none"> [0] Disable = Don't relay the Calling Party Category between SIP and PRI (default). [1] Enable = Calling Party Category is relayed between SIP and PRI. <p>If enabled, the Calling Party Category received in the OLI IE of an incoming SETUP is relayed to the From/P-Asserted-Id headers of the outgoing INVITE message and vice versa.</p> <p>For example: From:<sip:2000;cpc=payphone@10.8.23.70>;tag=1c1806157451</p> <p>Note: This feature is supported only when using NI-2 PRI variant.</p> |
| MLPP (Multi-level Precedence & Preemption) | |
| Call Priority Mode [CallPriorityMode] | <p>Enables Priority Calls handling.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> [0] Disable = Disable (default). [1] MLPP = Priority Calls handling is enabled. |

Table 5-27: Digital Gateway Parameters

| Parameter | Description |
|--|---|
| MLPP Default Namespace [MLPPDefaultNamespace] | <p>Determines the Namespace used for MLPP calls received from the ISDN side and destined for the Application Server. The Namespace value is not present in the Precedence IE of the PRI SETUP message. Therefore, the value is used in the Resource-Priority header of the outgoing SIP INVITE request. Valid options include:</p> <ul style="list-style-type: none"> ▪ [1] DSN = DSN (default) ▪ [2] DOD = DOD ▪ [3] DRSN = DRSN |
| Default Call Priority [SIPDefaultCallPriority] | <p>Defines the default call priority for MLPP calls. Valid options include:</p> <ul style="list-style-type: none"> ▪ [0] 0 = ROUTINE (default) ▪ [2] 2 = PRIORITY ▪ [6] 6 = IMMEDIATE ▪ [8] 8 = FLASH-OVERRIDE ▪ [9] 9 = FLASH-OVERRIDE-OVERRIDE <p>If the incoming SIP INVITE request doesn't contain a valid priority value in the Resource-Priority header, the default value is used in the Precedence IE (after translation to the relevant ISDN Precedence value) of the outgoing PRI SETUP message. If the incoming PRI SETUP message doesn't contain a valid Precedence Level value, the default value is used in the Resource-Priority header of the outgoing SIP INVITE request. In this scenario, the character string is sent without translation to a numerical value.</p> |
| MLPP DiffServ [MLPPDiffserv] | <p>Defines the DiffServ value (DSCP) used in IP packets containing SIP messages that are related to MLPP calls. The valid range is 0 to 63. The default value is 50.</p> |

5.5.10 Configuring the Advanced Applications

The **Advanced Applications** submenu enables you to configure advanced applications such as RADIUS.

5.5.10.1 Configuring RADIUS Accounting Parameters

The 'RADIUS Parameters' screen is used for configuring the Remote Authentication Dial In User Service (RADIUS) accounting parameters.

➤ **To configure the RADIUS parameters, take these 4 steps:**

1. Open the 'RADIUS Parameters' screen (**Protocol Management** menu > **Advanced Applications** submenu > **RADIUS Parameters**).

Figure 5-33: RADIUS Parameters Screen

| RADIUS Parameters | |
|---------------------------------------|--|
| ! Enable RADIUS | Disable <input type="button" value="v"/> |
| ! RADIUS Accounting Server IP Address | 0.0.0.0 |
| ! RADIUS Accounting Port | 1646 |
| RADIUS Accounting Type | At Call Release <input type="button" value="v"/> |
| AAA Indications | None <input type="button" value="v"/> |

2. Configure the RADIUS accounting parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-28: RADIUS Parameters

| Parameter | Description |
|---|---|
| Enable RADIUS [EnableRADIUS] | Enables or disables the RADIUS application. Valid options include: <ul style="list-style-type: none"> ▪ [0] Disables = disables RADIUS application (default) ▪ [1] Enable = enables RADIUS application |
| RADIUS Accounting Server IP Address [RADIUSAccServerIP] | IP address of the RADIUS accounting server. |
| RADIUS Accounting Port [RADIUSAccPort] | Port of the RADIUS accounting server. The default value is 1646. |
| RADIUS Accounting Type [RADIUSAccountingType] | Determines when the RADIUS accounting messages are sent to the RADIUS accounting server. Valid options include: <ul style="list-style-type: none"> ▪ [0] At Call Release = Sent at the release of the call only (default). ▪ [1] At Connect and Release = Sent at the connect and release of the call. ▪ [2] At Setup and Release = Sent at the setup and release of the call. |
| AAA Indications [AAAIndications] | Determines which Authentication, Authorization and Accounting (AAA) indications to use. Valid options include: <ul style="list-style-type: none"> ▪ [0] None = No indications (default). ▪ [3] Accounting Only = Only accounting indications are used. |

5.5.10.2 Configuring the FXO Parameters

The 'FXO Settings' screen is used to configure the gateway's specific FXO parameters.



Note: The 'FXO Settings' screen is only available for gateways providing FXO interface.

➤ **To configure the FXO parameters, take these 4 steps:**

1. Open the 'FXO Settings' screen (**Protocol Management** menu > **Advanced Applications** submenu > **FXO Settings** option).

Figure 5-34: FXO Settings Screen

| FXO Settings | |
|------------------------------------|---|
| Dialing Mode | Two Stages <input type="button" value="v"/> |
| Waiting for Dial Tone | No <input type="button" value="v"/> |
| Time to Wait before Dialing [msec] | 1000 |
| Ring Detection Timeout [sec] | 8 |
| Reorder Tone Duration [sec] | 255 |
| Answer Supervision | No <input type="button" value="v"/> |
| Rings before Detecting Caller ID | 1 <input type="button" value="v"/> |
| Send Metering Message to IP | No <input type="button" value="v"/> |
| Disconnect on Busy Tone | Yes <input type="button" value="v"/> |
| Disconnect On Dial Tone | Disable <input type="button" value="v"/> |
| Guard Time Between Calls | 1 |

2. Configure the FXO parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-29: FXO Parameters

| Parameter | Description |
|--|--|
| Dialing Mode [IsTwoStageDial] | <p>Used for IP→FXO modules calls.</p> <ul style="list-style-type: none"> [0] One Stage = One-stage dialing. [1] Two Stages = Two-stage dialing (default). <p>If two-stage dialing is enabled, then the FXO module seizes one of the PSTN/PBX lines without performing any dial, the remote user is connected over IP to PSTN/PBX, and all further signaling (dialing and Call Progress Tones) is performed directly with the PBX without the gateway's intervention.</p> <p>If one-stage dialing is enabled, then the FXO module seizes one of the available lines (according to the 'Channel Select Mode' parameter), and dials the destination phone number received in the INVITE message. Use the 'Waiting For Dial Tone' parameter to specify whether the dialing should come after detection of dial tone, or immediately after seizing of the line.</p> |
| Waiting For Dial Tone [IsWaitForDialTone] | <p>Used for IP→FXO module.</p> <ul style="list-style-type: none"> [0] No = Don't wait for dial tone. [1] Yes = Wait for dial tone (default). <p>When 'One Stage Dialing' is enabled and 'Waiting for Dial Tone' is enabled, the FXO module dials the phone number (to the PSTN/PBX line) only after it detects a dial tone.</p> <p>If 'Waiting For Dial Tone' is disabled, the FXO module immediately dials the phone number after seizing the PSTN/PBX line, without 'listening' to dial tone.</p> <p>Notes:</p> <ul style="list-style-type: none"> The correct dial tone parameters should be configured in the Call Progress Tones file. It can take the gateway 1 to 3 seconds to detect a dial tone (according to the dial tone configuration in the Call Progress Tones file). |
| Time to Wait before Dialing [msec] [WaitForDialTime] | <p>For Digital: Determines the delay after hook-flash is generated and dialing is begun. Applies to call transfer (TrunkTransferMode = 3) on CAS gateways.</p> <p>For Analog: Determines the delay before the gateway starts dialing on the FXO line in the following scenarios (applicable only to FXO modules):</p> <ul style="list-style-type: none"> The delay between the time the line is seized and dialing is begun, during the establishment of an IP→Tel call. Note: Applicable only to FXO modules for single stage dialing, when waiting for dial tone (IsWaitForDialTone) is disabled. The delay between the time when Wink is detected and dialing is begun, during the establishment of an IP→Tel call (for DID lines, EnabledDIDWink = 1). For call transfer. The delay after hook-flash is generated and dialing is begun. <p>The valid range (in milliseconds) is 0 to 20,000 (i.e., 20 seconds). The default value is 1,000 (i.e., 1 second).</p> |

Table 5-29: FXO Parameters

| Parameter | Description |
|--|---|
| Ring Detection Timeout [sec] [FXOBetweenRingTime] | <p>Note: Applicable only to FXO modules for Tel→IP calls.</p> <p>The Ring Detection timeout is used differently for normal and for automatic dialing.</p> <p>If automatic dialing is not used, and if Caller ID is enabled, then the FXO module seizes the line after detection of the second ring signal (allowing detection of caller ID, sent between the first and the second rings). If the second ring signal doesn't arrive for 'Ring Detection Timeout' the gateway doesn't initiate a call to IP.</p> <p>When automatic dialing is used, the FXO module initiates a call to IP when ringing signal is detected. The FXO line is seized only if the remote IP party answers the call. If the remote party doesn't answer the call and the ringing signal stops for 'Ring Detection Timeout', the FXO module Releases the IP call.</p> <p>Usually set to a value between 5 and 8. The default is 8 seconds.</p> |
| Reorder Tone Duration [sec] [TimeForReorderTone] | <p>For Analog: Busy or Reorder tone duration (seconds) the FXO module plays before releasing the line.</p> <p>The valid range is 0 to 100. The default is 0 seconds</p> <p>Usually, after playing a Reorder / Busy tone for the specified duration, the FXS module starts playing an Offhook Warning tone.</p> <p>Note 1: Selection of Busy or Reorder tone is performed according to the release cause received from IP.</p> <p>Note 2: Refer also to the parameter 'Enable Calls Cut Through' (CutThrough) (described in 'General Parameters' on page 103).</p> <p>For Digital: Busy or Reorder Tone duration the CAS gateway plays before releasing the line.</p> <p>The valid range is 0 to 15. The default value is 10 seconds.</p> <p>Applicable also to ISDN if PlayBusyTone2ISDN = 2. Selection of Busy or Reorder tone is done according to release cause received from IP.</p> |
| Answer Supervision [EnableVoiceDetection] | <ul style="list-style-type: none"> [1] Yes = FXO/CAS module sends 200 OK (to INVITE) messages when speech/fax/modem is detected. [0] No = 200 OK is sent immediately after the FXO/CAS module finishes dialing (default). <p>Usually this feature is used only when early media is used to establish voice path before the call is answered.</p> <p>Note: This feature is applicable only to 'One Stage' dialing for FXO modules.</p> |
| Rings before Detecting Caller ID [RingsBeforeCallerID] | <p>Sets the number of rings before the gateway starts detection of Caller ID (FXO only).</p> <ul style="list-style-type: none"> [0] 0 = Before first ring. [1] 1 = After first ring (default). [2] 2 = After second ring. |
| Send Metering Message to IP [SendMetering2IP] | N/A. |
| Disconnect on Busy Tone [DisconnectOnBusyTone] | <ul style="list-style-type: none"> [0] No = Do not disconnect call on detection of busy tone (FXO module). [1] Yes = Call is released (on FXO module) if busy or reorder (fast busy) tones are detected on the gateway's port (default). |

Table 5-29: FXO Parameters

| Parameter | Description |
|---|---|
| Disconnect on Dial Tone [DisconnectOnDialTone] | <p>FXO modules can disconnect a call after a dial tone from the PBX is detected.</p> <ul style="list-style-type: none">▪ [0] Disable = Call isn't released.▪ [1] Enable = Call is released if dial tone is detected on the gateway's FXO port (default). <p>Note: This option is in addition to the mechanism that disconnects a call when either busy or reorder tones are detected.</p> |
| Guard Time Between Calls [GuardTimeBetweenCalls] | <p>Defines the time interval (in seconds) after a call has ended and a new call can be accepted for IP to Tel calls. This is applicable only to FXO modules.</p> <p>The valid range is 0 to 10. The default value is 1 second.</p> <p>Note: Occasionally, after a call is ended and onhook is applied, a delay is required before placing a new call (and performing offhook). This is necessary to prevent wrong hook-flash detection or other glare phenomena.</p> |

5.5.10.3 Configuring the Voice Mail (VM) Parameters

The 'Voice Mail' screen is used to configure the Voice Mail (VM) parameters. The VM application applies only to FXO/CAS modules. For detailed information on VM, refer to the *CPE Configuration Guide for Voice Mail User's Manual*.

➤ **To configure the VM parameters, take these 4 steps:**

1. Open the 'Voice Mail' screen (**Protocol Management** menu > **Advanced Applications** submenu > **Voice Mail** option).

Figure 5-35: Voice Mail Screen

| Voice Mail | |
|--|-----------------|
| General | |
| Voice Mail Interface | DTMF |
| Line Transfer Mode | Semi Supervised |
| Digit Patterns | |
| Forward on Busy Digit Pattern (Internal) | |
| Forward on No Answer Digit Pattern (Internal) | |
| Forward on Do Not Disturb Digit Pattern (Internal) | |
| Forward on No Reason Digit Pattern (Internal) | |
| Forward on Busy Digit Pattern (External) | |
| Forward on No Answer Digit Pattern (External) | |
| Forward on Do Not Disturb Digit Pattern (External) | |
| Forward on No Reason Digit Pattern (External) | |
| Internal Call Digit Pattern | |
| External Call Digit Pattern | |
| Disconnect Call Digit Pattern | |
| MWI | |
| MWI Off Digit Pattern | |
| MWI On Digit Pattern | |
| MWI Suffix Pattern | |
| SMDI | |
| Enable SMDI | Disable |
| SMDI Timeout [msec] | 2000 |

2. Configure the Voice Mail parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-30: Voice Mail Parameters

| Parameter | Description |
|--|---|
| General | |
| Voice Mail Interface [VoiceMailInterface] | <p>Enables the VM application on the gateway and determines the communication method used between the PBX and the gateway.</p> <ul style="list-style-type: none"> ▪ [0] None (default) ▪ [1] DTMF ▪ [2] SMDI (N/A)[3] QSIG ▪ [4] SETUP Only (ISDN) |
| Line Transfer Mode [LineTransferMode] | <p>Determines the transfer method used by the gateway.</p> <ul style="list-style-type: none"> ▪ [0] None = IP (default). ▪ [1] Blind = PBX blind transfer. After receiving a REFER message from the IP side, the FXO sends a hook-flash to the PBX, dials the digits (that are received in the Refer-To header), and then immediately drops the line (on-hook). The PBX performs the transfer internally. ▪ [2] Semi Supervised = PBX Semi-Supervised transfer. After receiving a REFER message from the IP side, the FXO sends a hook-flash to the PBX, and then dials the digits (that are received in the Refer-To header). If no Busy or Reorder tones are detected (within approximately 2 seconds), the gateway completes the call transfer by releasing the line; otherwise, the transfer is cancelled, the gateway sends a SIP NOTIFY message with a failure reason in the NOTIFY body (such as 486 if busy tone detected), and generates an additional hook-flash towards the FXO line to restore connection to the original call. ▪ [3] Supervised = PBX Supervised transfer. After receiving a REFER message from the IP side, the FXO sends a hook-flash to the PBX, and then dials the digits (that are received in the Refer-To header). The FXO waits for connection of the transfer call and if speech is detected (e.g., "hello") within approximately 2 seconds, the gateway completes the call transfer by releasing the line; otherwise, the transfer is cancelled, the gateway sends a SIP NOTIFY message with a failure reason in the NOTIFY body (such as 486 if busy tone detected), and generates an additional hook-flash towards the FXO line to restore connection to the original call. <p>For additional information, refer to the CPE SIP Configuration Guide for IP Voice Mail.</p> <p>Note: Applicable only for FXO interfaces and CAS protocols.</p> |
| Digit Patterns The following digit pattern parameters apply only to VM applications that use the DTMF communication method. For the available patterns' syntaxes, refer to the CPE Configuration Guide for Voice Mail. | |
| Forward on Busy Digit Pattern (Internal) [DigitPatternForwardOnBusy] | <p>Determines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an internal extension.</p> <p>The valid range is a 120-character string.</p> |

Table 5-30: Voice Mail Parameters

| Parameter | Description |
|--|--|
| Forward on No Answer Digit Pattern (Internal) [DigitPatternForwardOnNoAnswer] | Determines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an internal extension. The valid range is a 120-character string. |
| Forward on Do Not Disturb Digit Pattern (Internal) [DigitPatternForwardOnDND] | Determines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an internal extension. The valid range is a 120-character string. |
| Forward on No Reason Digit Pattern (Internal) [DigitPatternForwardNoReason] | Determines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an internal extension. The valid range is a 120-character string. |
| Forward on Busy Digit Pattern (External) [DigitPatternForwardOnBusyExt] | Determines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an external line and not an internal extension. The valid range is a 120-character string. |
| Forward on No Answer Digit Pattern (External) [DigitPatternForwardOnNoAnswerExt] | Determines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an external line and not an internal extension. The valid range is a 120-character string. |
| Forward on Do Not Disturb Digit Pattern (External) [DigitPatternForwardOnDNDExt] | Determines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an external line and not an internal extension. The valid range is a 120-character string. |
| Forward on No Reason Digit Pattern (External) [DigitPatternForwardNoReasonExt] | Determines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an external line and not an internal extension. The valid range is a 120-character string. |
| Internal Call Digit Pattern [DigitPatternInternalCall] | Determines the digit pattern used by the PBX to indicate an internal call. The valid range is a 120-character string. |
| External Call Digit Pattern [DigitPatternExternalCall] | Determines the digit pattern used by the PBX to indicate an external call. The valid range is a 120-character string. |
| Disconnect Call Digit Pattern [TelDisconnectCode] | Determines a digit pattern that, when received from the Tel side, indicates the gateway to disconnect the call. The valid range is a 25-character string. |
| MWI | |
| MWI Off Digit Pattern [MWIOffCode] | Determines a digit code used by the gateway to notify the PBX that there aren't any messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string. |
| MWI On Digit Pattern [MWIONCode] | Determines a digit code used by the gateway to notify the PBX of messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string. |

Table 5-30: Voice Mail Parameters

| Parameter | Description |
|---------------------------------------|--|
| MWI Suffix Pattern [MWISuffixCode] | Determines a digit code used by the gateway as a suffix for MWIOnCode and MWIOffCode. This suffix is added to the generated DTMF string after the extension number. The valid range is a 25-character string. |
| SMDI (currently not supported) | |
| Enable SMDI [SMDI] | N/A |
| SMDI Timeout [SMDITimeOut] | N/A |

5.5.11 Configuring the IPmedia Parameters

The 'IPmedia Parameters' screen is used to configure the media parameters. For detailed information on each parameter, refer to 'Media Server Parameters' on page 337.

➤ **To configure the IPmedia parameters, take these 4 steps:**

1. Open the 'IPmedia Parameters' screen (**Protocol Management** menu > **IPMedia Parameters**).

Figure 5-36: IPmedia Parameters Screen

| IPmedia Parameters | |
|----------------------------------|-----------|
| ! Number of Media Channels | 20 |
| Enable Voice Streaming | Enable ▼ |
| NetAnn Announcement ID | annc |
| MSCML ID | mscml |
| Conference | |
| Conference ID | conf |
| Bip On Conference | Enable ▼ |
| Enable DTMF Clamping | Enable ▼ |
| Enable Conference DTMF Reporting | Disable ▼ |

2. Configure the IPmedia parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-31: IPmedia Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|--|
| Number of Media Channels [MediaChannels] | The number of DSP channels that are allocated for IP conferences, IP streaming and IP Transcoding (other DSP channels can be used for PSTN Gateway). The maximum value of Media Channels depends on the number of installed Media Processing modules (MPM): 1 module = 20 channels; 2 modules = 60; 3 modules = 100. The default value is 0. |
| Enable Voice Streaming [EnableVoiceStreaming] | Enables/disables the HTTP Voice Streaming application (play / record). <ul style="list-style-type: none"> [0] Disable = Voice Streaming is disabled (default). [1] Enable = Voice Streaming is enabled. |
| NetAnn Announcement ID [NetAnnAnncID] | NetAnn identification string (up to 16 characters), used to play an announcement using the NetAnn interface. The application server sends a regular SIP INVITE message with SIP URI that includes this identifier string and a "play=" parameter that identifies the necessary announcement. The default value is 'annc'. Example 1: INVITE sip: annc@10.2.3.4;play=http://localhost/1. Example 2: INVITE sip: annc@10.2.3.4;play=http://10.2.3.4/Annc/hello.wav. |
| MSCML ID [MSCMLID] | MSCML identification string (up to 16 characters). To start an MSCML session the application server sends a regular SIP INVITE message with a SIP URI that includes this string. The default value is 'ivr'. For example: INVITE sip:ivr@10.2.3.4 Subsequent INFO message(s) carry the requests and responses. |
| Transcoding ID [TranscodingID] | Transcoding identification string (up to 16 characters), used for identifying an incoming Transcoding call. The default value is 'trans'. For detailed information on Transcoding, refer to 'NetAnn Interface' on page 463. |
| Conference | |
| Conference ID [ConferenceID] | Conference Identification string (up to 16 characters). The default value is 'conf'. For example: ConferenceID = MyConference Note: To join a conference, the INVITE URI must include the Conference ID string, preceded by the number of the participants in the conference, and terminated by a unique number. For example: Invite sip:4MyConference1234@10.1.10.10. INVITE messages with the same URI join the same conference. |
| Beep upon New Participant in Conference [BipOnConference] | Configure this parameter for a beep to be played when a new participant joins a conference and when a participant leaves a conference (in the latter case, a beep of a different pitch is heard). <ul style="list-style-type: none"> [0] Disable = Beep is disabled. [1] Enable = Beep is enabled (default). |

Table 5-31: IPmedia Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| Enable DTMF Clamping [EnableConferenceDTMFClamp] | Determines the gateway logic once a DTMF is received on any conference participant. If enabled, the DTMF is not regenerated towards the other conference participants. This logic is only relevant for simple (NetAnn) Conferencing. <ul style="list-style-type: none">▪ [0] Disable = Disable▪ [1] Enable = Enable (default) |
| Enable Conference DTMF Reporting [EnableConferenceDTMFReporting] | Determines the media server logic once a DTMF is received on any conference participant. If enabled, the gateway reports this DTMF in an out-of-band SIP message (according to TxDTMFOptions). This logic is only relevant for simple (NetAnn) Conferencing. <ul style="list-style-type: none">▪ [0] Disable = Disable (default)▪ [1] Enable = Enable |

5.6 Network Settings

The **Network Settings** menu allows you to configure the following:

- IP Settings (refer to 'Configuring the IP Settings' on page 178)
- Application Settings (refer to 'Configuring the Application Settings' on page 182)
- NFS Settings (refer to 'Configuring the NFS Settings' on page 184)
- IP Routing Table (refer to 'Configuring the IP Routing Table' on page 186)
- VLAN Settings (refer to 'Configuring the VLAN Settings' on page 188)

5.6.1 Configuring the IP Settings

The 'IP Settings' screen is used for configuring various IP networking parameters.

➤ **To configure the IP Settings parameters, take these 4 steps:**

1. Open the 'IP Settings' screen (**Advanced Configuration** menu > **Network Settings** > **IP Settings** option).

Figure 5-37: IP Settings Screen

| IP Settings | |
|-------------------------|--|
| IP Networking Mode | Single IP Network <input type="button" value="v"/> |
| IP Address | 10.33.4.128 |
| Subnet Mask | 255.255.0.0 |
| Default Gateway Address | 10.33.0.1 |
| DNS Settings | |
| DNS Primary Server IP | |
| DNS Secondary Server IP | |
| DHCP Settings | |
| Enable DHCP | Disable <input type="button" value="v"/> |
| NAT Settings | |
| ! NAT IP Address | 0.0.0.0 |
| Differential Services | |
| Network QoS | 48 |
| Media Premium QoS | 46 |
| Control Premium QoS | 46 |
| Gold QoS | 26 |
| Bronze QoS | 10 |

2. Configure the IP Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-32: Network Settings -- IP Settings Parameters

| Parameter | Description |
|--|--|
| IP Networking Mode [EnableMultipleIPs] | <p>Enables / disables the Multiple IPs mechanism.</p> <ul style="list-style-type: none"> ▪ [0] Single IP Network = Single IP network (default). ▪ [1] Multiple IP Network = Multiple IP networks. ▪ [1] Dual IP (Media & Control) = Multiple IP networks. ▪ [1] Dual IP (OAM & Control) = Multiple IP networks. ▪ [1] Dual IP (OAM & Medial) = Multiple IP networks. <p>For detailed information on Multiple IPs, refer to 'Multiple IPs' on page 431.</p> |
| IP Address | <p>IP address of the gateway. Enter the IP address in dotted format notation, for example 10.8.201.1.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ A warning message is displayed (after clicking the button Submit) if the entered value is incorrect. ▪ After changing the IP address you must reset the gateway. |
| Subnet Mask | <p>Subnet mask of the gateway. Enter the subnet mask in dotted format notation, for example 255.255.0.0</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ A warning message is displayed (after clicking the button Submit) if the entered value is incorrect. ▪ After changing the subnet mask, the gateway must be reset. |
| Default Gateway Address | <p>IP address of the default gateway used by the gateway. Enter the IP address in dotted format notation, for example 10.8.0.1.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ A warning message is displayed (after clicking the button Submit) if the entered value is incorrect. ▪ After changing the default gateway IP address, the gateway must be reset. <p>For detailed information on multiple routers support, refer to 'Multiple Routers Support' on page 429.</p> |
| OAM Network Settings (available only in Multiple IPs and Dual IP modes) | |
| IP Address [LocalOAMIPAddress] | <p>The gateway's source IP address in the OAM network. The default value is 0.0.0.0.</p> |
| Subnet Mask [LocalOAMSubnetMask] | <p>The gateway's subnet mask in the OAM network. The default subnet mask is 0.0.0.0.</p> |
| Default Gateway Address [LocalOAMDefaultGW] | <p>N/A. Use the IP Routing table instead (refer to 'Configuring the IP Routing Table' on page 186).</p> |

Table 5-32: Network Settings -- IP Settings Parameters

| Parameter | Description |
|--|--|
| Control Network Settings (available only in Multiple IPs and Dual IP modes) | |
| IP Address [LocalControlIPAddress] | The gateway's source IP address in the Control network. The default value is 0.0.0.0. |
| Subnet Mask [LocalControlSubnetMask] | The gateway's subnet mask in the Control network. The default subnet mask is 0.0.0.0. |
| Default Gateway Address [LocalControlDefaultGW] | N/A. Use the IP Routing table instead (refer to 'Configuring the IP Routing Table' on page 186). |
| Media Network Settings (available only in Multiple IPs and Dual IP modes) | |
| IP Address [LocalMediaIPAddress] | The gateway's source IP address in the Media network. The default value is 0.0.0.0. |
| Subnet Mask [LocalMediaSubnetMask] | The gateway's subnet mask in the Media network. The default subnet mask is 0.0.0.0. |
| Default Gateway Address [LocalMediaDefaultGW] | The gateway's default gateway IP address in the Media network. The default value is 0.0.0.0. |
| DNS Settings | |
| DNS Primary Server IP [DNSPriServerIP] | IP address of the primary DNS server. Enter the IP address in dotted format notation, for example 10.8.2.255. Note: To use Fully Qualified Domain Names (FQDN) in the Tel to IP Routing table, you must define this parameter. |
| DNS Secondary Server IP [DNSSecServerIP] | IP address of the second DNS server. Enter the IP address in dotted format notation, for example 10.8.2.255. |
| DHCP Settings | |
| Enable DHCP [DHCPEnable] | <ul style="list-style-type: none"> [0] Disable = Disable DHCP support on the gateway (default). [1] Enable = Enable DHCP support on the gateway. <p>After the gateway is powered up, it attempts to communicate with a BootP server. If a BootP server is not responding and if DHCP is enabled, then the gateway attempts to get its IP address and other network parameters from the DHCP server.</p> <p>Notes:</p> <ul style="list-style-type: none"> After you enable the DHCP Server (using the Embedded Web Server) follow this procedure: <ol style="list-style-type: none"> Click the Submit button. Save the configuration (refer to 'Saving Configuration' on page 278). Reset the gateway <i>directly</i> (reset via Embedded Web Server doesn't trigger the BootP/DHCP procedure and the parameter DHCPEnable reverts to 0). Throughout the DHCP procedure the BootP/TFTP application must be deactivated. Otherwise, the gateway receives a response from the BootP server instead of the DHCP server. For additional information on DHCP, refer to the <i>SIP Series Reference Manual</i>. The DHCPEnable is a special 'Hidden' parameter. Once defined and saved in flash memory, its assigned value doesn't revert to its default even if the parameter doesn't appear in the <i>ini</i> file. |

Table 5-32: Network Settings -- IP Settings Parameters

| Parameter | Description |
|--|--|
| NAT Settings | |
| NAT IP Address [StaticNatIP] | Global gateway IP address. Define if static Network Address Translation (NAT) device is used between the gateway and the Internet. |
| Differential Services. For detailed information on IP QoS via Differentiated Services, refer to 'IP QoS via Differentiated Services (DiffServ)' on page 430. | |
| Network QoS [NetworkServiceClassDiffServ] | Sets the DiffServ value for Network service class content. The valid range is 0 to 63. The default value is 48. |
| Media Premium QoS [PremiumServiceClassMediaDiffServ] | Sets the DiffServ value for Premium Media service class content (only if IPDiffServ is not set in the selected IP Profile). The valid range is 0 to 63. The default value is 46. Note: The value for the Premium Control DiffServ is determined by (according to priority): (1) IPDiffServ value in the selected IP Profile. (2) PremiumServiceClassMediaDiffServ. |
| Control Premium QoS [PremiumServiceClassControlDiffServ] | Sets the DiffServ value for Premium Control service class content (only if ControlIPDiffServ is not set in the selected IP Profile). The valid range is 0 to 63. The default value is 40. Note: The value for the Premium Control DiffServ is determined by (according to priority): (1) ControlIPDiffServ value in the selected IP Profile. (2) PremiumServiceClassControlDiffServ. |
| Gold QoS [GoldServiceClassDiffServ] | Sets the DiffServ value for the Gold service class content. The valid range is 0 to 63. The default value is 26. |
| Bronze QoS [BronzeServiceClassDiffServ] | Sets the DiffServ value for the Bronze service class content. The valid range is 0 to 63. The default value is 10. |

5.6.2 Configuring the Application Settings

The 'Application Settings' screen is used for configuring various application parameters (e.g., for Telnet).

- **To configure the Application Settings parameters, take these 4 steps:**

 1. Open the 'Application Settings' screen (**Advanced Configuration** menu > **Network Settings** > **Application Settings** option).

Figure 5-38: Application Settings Screen

| Application Settings | |
|------------------------------|--------------------|
| NTP Settings | |
| NTP Server IP Address | 0.0.0.0 |
| NTP UTC Offset | Hours 0 Minutes 0 |
| NTP Update Interval | Hours 24 Minutes 0 |
| Telnet Settings | |
| ! Embedded Telnet Server | Disable |
| ! Telnet Server TCP Port | 23 |
| ! Telnet Server Idle Timeout | 0 |
| SSH Server Enable | Disable |
| SSH Server Port | 22 |
| STUN Settings | |
| Enable STUN | Disable |
| STUN Server Primary IP | 0.0.0.0 |
| STUN Server Secondary IP | 0.0.0.0 |
| NFS Settings | |
| NFS Table | --> |

2. Configure the Application Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-33: Network Settings, Application Settings Parameters

| Parameter | Description |
|---|---|
| NTP Settings | |
| For detailed information on Network Time Protocol (NTP), refer to 'Simple Network Time Protocol Support' on page 430. | |
| NTP Server IP Address [NTPServerIP] | IP address (in dotted format notation) of the NTP server. The default IP address is 0.0.0.0 (the internal NTP client is disabled). |
| NTP UTC Offset [NTPServerUTCOffset] | Defines the UTC (Universal Time Coordinate) offset (in seconds) from the NTP server. The default offset is 0. The offset range is -43200 to 43200 seconds. |
| NTP Update Interval [NTPUpdateInterval] | Defines the time interval (in seconds) the NTP client requests for a time update. The default interval is 86400 seconds (24 hours). The range is 0 to 214783647 seconds. Note: It isn't recommended to be set beyond one month (2592000 seconds). |
| Telnet Settings | |
| Embedded Telnet Server [TelnetServerEnable] | Enables or disables the embedded Telnet server. Telnet is disabled by default for security reasons. <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable (Unsecured). ▪ [2] Enable Secured (SSL). |
| Telnet Server TCP Port [TelnetServerPort] | Defines the port number for the embedded Telnet server. The valid range is all valid port numbers. The default port is 23. |
| Telnet Server Idle Timeout [TelnetServerIdleDisconnect] | Sets the timeout for disconnection of an idle Telnet session (in minutes). When set to zero, idle sessions are not disconnected. The valid range is any value. The default value is 0. |
| SSH Server Enable [SSHServerEnable] | Enables or disables the embedded Secure SHell (SSH) server. <ul style="list-style-type: none"> ▪ [0] Disable = Disable SSH server (default) ▪ [1] Enable = Enable |
| SSH Server Port [SSHServerPort] | Defines the port number for the embedded SSH server. Range is any valid port number. Default is port 23. |

Table 5-33: Network Settings, Application Settings Parameters

| Parameter | Description |
|---|--|
| STUN Settings | |
| Enable STUN [EnableSTUN] | <ul style="list-style-type: none"> ▪ [0] Disable = STUN protocol is disabled (default). ▪ [1] Enable = STUN protocol is enabled. <p>When enabled, the gateway functions as a STUN client and communicates with a STUN server located in the public Internet. STUN is used to discover whether the gateway is located behind a NAT and the type of that NAT. In addition, it is used to determine the IP addresses and port numbers that the NAT assigns to outgoing signaling messages (using SIP) and media streams (using RTP, RTCP and T.38). STUN works with many existing NAT types, and does not require any special behavior from them.</p> <p>This parameter cannot be changed on-the-fly and requires a gateway reset.</p> <p>For detailed information on STUN, refer to 'STUN' on page 425.</p> <p>Note: For defining the STUN server domain name, use the <i>ini</i> file parameter STUNServerDomainName (refer to 'Networking Parameters' on page 299).</p> |
| STUN Server Primary IP [STUNServerPrimaryIP] | <p>Defines the IP address of the primary STUN server.</p> <p>The valid range is the legal IP addresses. The default value is 0.0.0.0.</p> |
| STUN Server Secondary IP [STUNServerSecondaryIP] | <p>Defines the IP address of the secondary STUN server.</p> <p>The valid range is the legal IP addresses. The default value is 0.0.0.0.</p> |
| NFS Settings | |
| NFS Table | <p>For detailed information on configuring the NFS table, refer to 'Configuring the NFS Settings' on page 184.</p> |

5.6.3 Configuring the NFS Settings

Network File System (NFS) enables the gateway to access a remote server's shared files and directories and to handle them as if they're located locally. A file system, the NFS is independent of machine types, OSs, and network architectures. Up to five different NFS file systems can be configured.

NFS is utilized by the gateway to load the *cmp*, *ini* and configuration files via the Automatic Update mechanism (refer to 'Automatic Update Mechanism' on page [266](#)).

Note that an NFS file server can share multiple file systems. There must be a separate row for each remote file system shared by the NFS file server that needs to be accessed by the gateway.

➤ **To configure the NFS Settings parameters, take these 7 steps:**

1. Open the 'Application Settings' screen (**Advanced Configuration** menu > **Network Settings** > **Application Settings** option); the 'Application Settings' screen is displayed (refer to 'Configuring the Application Settings' on page 182).
2. Open the 'NFS Settings' screen by clicking the **NFS Table** arrow sign (-->).

Figure 5-39: NFS Settings Screen

| Edit | Line Number | Host / IP | Root Path | NFS Version | Auth Type | UID | GID | VLAN Type |
|----------------------------------|-------------|-----------|----------------|-------------|-----------|-----|-----|-----------|
| <input checked="" type="radio"/> | 0 | 10.3.3.63 | /PROV_data/GW/ | 3 | Auth UNIX | 0 | 1 | MEDIA |

Line Number: 0

Add an Empty Line

3. To add a remote NFS file system, select an available line number from the 'Line Number' drop-down list.
4. Click the **Add an Empty Line** button; an empty line appears.
5. Configure the NFS Settings according to the table below.
6. Click the **Apply New Settings** button; the remote NFS file system is mounted immediately. Check the Syslog server for the 'NFS mount was successful' message.
7. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.



Note: To avoid terminating calls in progress, a row must not be deleted or modified while the blade is currently accessing files on that remote NFS file system.

➤ **To delete a remote NFS file system, take these 3 steps:**

1. Select the **Edit** radio button for the row to be deleted.
2. Click the **Delete Line** button; the row is deleted.
3. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

➤ **To modify an existing remote NFS file system, take these 4 steps:**

1. Select the **Edit** radio button for the row to be modified.
2. Change the values on the selected row according to your requirements.
3. Click the **Apply New Settings** button; the remote NFS file system is mounted using the new settings. Check the Syslog server for the 'NFS mount was successful' message.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-34: Network Settings -- NFS Settings Parameters

| Parameter | Description |
|--|--|
| Line Number [NFSServers_Index] | The row index of the remote file system. The valid range is 0 to 4. |
| Host / IP [NFSServers_HostOrIP] | The domain name or IP address of the NFS server. If a domain name is provided, a DNS server must be configured. |
| Root Path [NFSServers_RootPath] | Path to the root of the remote file system in the format: '/' + [path]. For example, /audio. |
| The combination of Host / IP and Root Path must be unique for each row in the table. For example, there must be only one row in the table with a Host / IP of 192.168.1.1 and Root Path of /audio. | |
| NFS Version [NFSServers_NfsVersion] | NFS version to use with the remote file system, 2 or 3 (default). |
| Auth Type [NFSServers_AuthType] | Identifies the authentication method used with the remote file system. <ul style="list-style-type: none"> [0] Auth NULL. [1] Auth UNIX (default). |
| UID [NFSServers_UID] | User ID used in authentication if using Auth UNIX. The valid range is 0 to 65537. The default is 0. |
| GID [NFSServers_GID] | Group ID used in authentication if using Auth UNIX. The valid range is 0 to 65537. The default is 1 |
| VLAN Type [NFSServers_VlanType] | The VLAN, OAM [0] or MEDIA [1], to use when accessing the remote file system. The default is to use the media VLAN. This parameter applies only if VLANs are enabled or if Multiple IPs is configured (refer to 'VLANS and Multiple IPs' on page 431). |

Below shows an example of an NFS table definition via *ini* file using parameter tables (for information on *ini* file parameter tables, refer to 'Configuring Parameter Tables Using the ini File' on page 295).

```
[NFSServers]
FORMAT NFSServers Index = NFSServers HostOrIP,
NFSServers RootPath, NFSServers NfsVersion, NFSServers AuthType,
NFSServers_UID, NFSServers_GID, NFSServers_VlanType;
NFSServers 1 = 101.1.13, /audio1, 3, 1, 0, 1, 1;
[\\NFSServers]
```

5.6.4 Configuring the IP Routing Table

The 'IP Routing Table' screen is used by the gateway to determine IP routing rules. It can be used, for example, to define static routing rules for the OAM and Control networks since a default gateway isn't supported for these networks (refer to 'Multiple IPs' on page 431). Before sending an IP packet, the gateway searches this table for an entry that matches the requested destination host / network. If such an entry is found, the gateway sends the packet to the indicated router. If no explicit entry is found, the packet is sent to the default gateway (configured in the 'IP Settings' screen -- refer to 'Configuring the IP Settings' on page 178). Up to 50 routing entries are available.

➤ **To configure the IP Routing table, take these 3 steps:**

1. Open the 'IP Routing Table' screen (**Advanced Configuration** menu > **Network Settings** > **Routing Table** option).

Figure 5-40: IP Routing Table Screen

| IP Routing Table | | | | | | | |
|----------------------------|------------------------|------------------|--------------------|------------|-----------|-----------|--|
| Delete Row | Destination IP Address | Destination Mask | Gateway IP Address | TTL | Hop Count | Interface | |
| 1 <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | 10.8.0.1 | 2147483647 | 1 | OAM | |
| 2 <input type="checkbox"/> | 10.8.0.0 | 255.255.0.0 | 10.8.23.138 | 2147483647 | 0 | OAM | |
| 3 <input type="checkbox"/> | 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 2147483647 | 1 | OAM | |
| 4 <input type="checkbox"/> | 127.0.0.1 | 255.255.255.255 | 127.0.0.1 | 2147483647 | 0 | OAM | |

Delete Selected Entries

Add a new table entry:

| Destination IP Address | Destination Mask | Gateway IP Address | Hop Count | Network Type |
|------------------------|----------------------|----------------------|-----------|--------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | 0 | OAM |

Note: All fields should have a value

Add New Entry

2. Use the 'Add a new table entry' pane to add a new routing rule. Each field in the IP routing table is described in the table below.
3. Click the button **Add New Entry**; the new routing rule is added to the IP routing table.

Table 5-35: IP Routing Table Column Description

| Column Name [ini File Parameter Name] | Description |
|---|--|
| Delete Row | To delete IP routing rules from the IP Routing Table, check the Delete Row check box in the rows of the routing rules you want to delete and click the button Delete Selected Entries ; the routing rules are removed from the table. |
| Destination IP Address [RoutingTableDestinationsColumn] | Specifies the IP address of the destination host / network. |
| Destination Mask [RoutingTableDestinationMasksColumn] | Specifies the subnet mask of the destination host / network. |
| <p>The address of the host / network you want to reach is determined by an AND operation that is applied on the fields 'Destination IP Address' and 'Destination Mask'.</p> <p>For example:</p> <p>To reach the network 10.8.x.x, enter 10.8.0.0 in the field 'Destination IP Address' and 255.255.0.0 in the field 'Destination Mask'. As a result of the AND operation, the value of the last two octets in the field 'Destination IP Address' is ignored.</p> <p>To reach a specific host, enter its IP address in the field 'Destination IP Address' and 255.255.255.255 in the field 'Destination Mask'.</p> | |

Table 5-35: IP Routing Table Column Description

| Column Name [ini File Parameter Name] | Description |
|--|---|
| Gateway IP Address [RoutingTableGatewaysColumn] | Specifies the IP address of the router to which the packets are sent if their destination matches the rules in the adjacent columns. |
| TTL | A read-only field that indicates the time period for which the specific routing rule is valid. The lifetime of a static route is infinite. |
| Hop Count [RoutingTableHopsCountColumn] | The maximum number of allowed routers between the gateway and destination. |
| Network Type [RoutingTableInterfacesColumn] | <p>Specifies the network type the routing rule is applied to.</p> <ul style="list-style-type: none"> ▪ [0] OAM (default). ▪ [1] Control. ▪ [2] Media. <p>For detailed information on the network types, refer to 'Multiple IPs' on page 431.</p> |

5.6.5 Configuring the VLAN Settings

For detailed information on the gateway VLAN implementation, refer to 'VLANs and Multiple IPs' on page 431.

➤ **To configure the VLAN Settings parameters, take these 4 steps:**

1. Open the 'VLAN Settings' screen (**Advanced Configuration** menu > **Network Settings** > **VLAN Settings** option).

Figure 5-41: VLAN Settings Screen

| VLAN Settings | |
|--------------------------|---------|
| VLAN Mode | Disable |
| ID Settings | |
| Native VLAN ID | 1 |
| OAM VLAN ID | 1 |
| Control VLAN ID | 2 |
| Media VLAN ID | 3 |
| Priority Settings | |
| Network Priority | 7 |
| Media Premium Priority | 6 |
| Control Premium Priority | 6 |
| Gold Priority | 4 |
| Bronze Priority | 2 |

2. Configure the VLAN Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-36: Network Settings -- VLAN Settings Parameters

| Parameter | Description |
|--|---|
| VLAN Mode [VLANMode] | <p>Sets the VLAN functionality.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable. ▪ [2] PassThrough = N/A. <p>Note: This parameter cannot be changed on-the-fly and requires a gateway reset.</p> |
| IP Settings | |
| Native VLAN ID [VLANNativeVlanID] | Sets the native VLAN identifier (PVID, Port VLAN ID). The valid range is 1 to 4094. The default value is 1. |
| OAM VLAN ID [VLANOamVlanID] | Sets the OAM (Operation, Administration and Management) VLAN identifier. The valid range is 1 to 4094. The default value is 1. |
| Control VLAN ID [VLANControlVlanID] | Sets the control VLAN identifier. The valid range is 1 to 4094. The default value is 2. |
| Media VLAN ID [VLANMediaVlanID] | Sets the media VLAN identifier. The valid range is 1 to 4094. The default value is 3. |
| Priority Settings | |
| Network Priority [VLANNetworkServiceClassPriority] | Sets the priority for Network service class content. The valid range is 0 to 7. The default value is 7. |
| Media Premium Priority [VLANPremiumServiceClassMediaPriority] | Sets the priority for the Premium service class content and media traffic. The valid range is 0 to 7. The default value is 6. |
| Control Premium Priority [VLANPremiumServiceClassControlPriority] | Sets the priority for the Premium service class content and control traffic. The valid range is 0 to 7. The default value is 6. |
| Gold Priority [VLANGoldServiceClassPriority] | Sets the priority for the Gold service class content. The valid range is 0 to 7. The default value is 4. |
| Bronze Priority [VLANBronzeServiceClassPriority] | Sets the priority for the Bronze service class content. The valid range is 0 to 7. The default value is 2. |

5.7 Media Settings

The **Media Settings** submenu is used to configure the gateway's channel parameters. These parameters are applied to all the gateway's channels.

From the **Media Settings** submenu, you can define the following:

- Voice Settings (refer to 'Configuring the Voice Settings' on page [191](#))
- Fax / Modem / CID Settings (refer to 'Configuring the Fax / Modem / CID Settings' on page [194](#))
- RTP/RTCP Settings (refer to 'Configuring the RTP / RTCP Settings' on page [198](#))
- Hook-Flash Settings (refer to 'Configuring the Hook-Flash Settings' on page [204](#))
- General Media Settings (refer to 'Configuring the General Media Settings' on page [205](#))



Notes:

- Parameters contained within square brackets are the names used to configure the parameters via the *ini* file.
- Channel parameters are changeable on-the-fly. Changes take effect from next call.
- Several Channels Settings parameters can be configured per call using profiles (refer to 'Configuring the Profile Definitions' on page [144](#)).
- The parameter 'Fax Transport Mode' (Fax / Modem / CID Settings screen) is overridden by the parameter `IsFaxUsed`.

5.7.1 Configuring the Voice Settings

The 'Voice Settings' screen is used for configuring various voice parameters such as voice volume.

➤ **To configure the Voice Settings parameters, take these 4 steps:**

1. Open the 'Voice Settings' screen (**Advanced Configuration** menu > **Media Settings** > **Voice Settings** option).

| Voice Settings | |
|--------------------------------|--------------------|
| Voice Volume (-32 to 31 dB) | 0 |
| Input Gain (-32 to 31 dB) | 0 |
| Silence Suppression | Disable |
| Echo Canceled | On |
| DTMF Transport Type | RFC2833 Relay DTMF |
| MF Transport Type | RFC2833 Relay MF |
| DTMF Volume (-31 to 0 dB) | -11 |
| Enable Answer Detector | Disable |
| Answer Detector Activity Delay | 0 |
| Answer Detector Silence Time | 10 |
| Answer Detector Redirection | Disable |
| Answer Detector Sensitivity | 0 |
| CAS Transport Type | CAS Events Only |
| ! DTMF generation twist | 0 |

2. Configure the Voice Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-37: Media Settings, Voice Settings Parameters

| Parameter | Description |
|-------------------------------|---|
| Voice Volume [VoiceVolume] | Voice gain control in dB. This parameter sets the level for the transmitted (IP→PSTN/Tel) signal. The valid range is -32 to 31 dB. The default value is 0 dB. |
| Input Gain [InputGain] | PCM input gain control in dB. This parameter sets the level for the received (Tel/PSTN→IP) signal. The valid range is -32 to 31 dB. The default value is 0 dB. |

Table 5-37: Media Settings, Voice Settings Parameters

| Parameter | Description |
|--|--|
| Silence Suppression [EnableSilenceCompression] | <p>Silence Suppression is a method conserving bandwidth on VoIP calls by not sending packets when silence is detected.</p> <ul style="list-style-type: none"> [0] Disable = Silence Suppression disabled (default). [1] Enable = Silence Suppression enabled. [2] Enable without Adaptation = A single silence packet is sent during silence period (applicable only to G.729). <p>Note: If the selected coder is G.729, the following rules determine the value of the 'annexb' parameter of the fmtp attribute in the SDP:</p> <ul style="list-style-type: none"> EnableSilenceCompression = 0 → 'annexb=no'. EnableSilenceCompression = 1 → 'annexb=yes'. EnableSilenceCompression = 2 and IsCiscoSCEMode = 0 → 'annexb=yes'. EnableSilenceCompression = 2 and IsCiscoSCEMode = 1 → 'annexb=no'. |
| Echo Canceller [EnableEchoCanceller] | <ul style="list-style-type: none"> [0] Off = Echo Canceller disabled. [1] On = Echo Canceller enabled (default). <p>Note: The parameter ECE is used to maintain backward compatibility.</p> |
| DTMF Transport Type [DTMFTransportType] | <ul style="list-style-type: none"> [0] DTMF Mute = Erase digits from voice stream, do not relay to remote. [2] Transparent DTMF = Digits remain in voice stream. [3] RFC 2833 Relay DTMF = Erase digits from voice stream, relay to remote according to RFC 2833 (default). [7] RFC 2833 Relay Rcv Mute = DTMFs are sent according to RFC 2833 and muted when received. <p>Note: This parameter is automatically updated if one of the following parameters is configured: TxDTMFOption or RxDTMFOption.</p> |
| MF Transport Type [MFTransportType] | N/A. |
| DTMF Volume (-31 to 0 dB) [DTMFVolume] | DTMF gain control value in dB (to the TDM analog side). The valid range is -31 to 0 dB. The default value is -11 dB. |
| Enable Answer Detector [EnableAnswerDetector] | N/A. |
| Answer Detector Activity Delay [AnswerDetectorActivityDelay] | N/A. |
| Answer Detector Silence Time [AnswerDetectorSilenceTime] | N/A. |
| Answer Detector Redirection [AnswerDetectorRedirection] | N/A. |

Table 5-37: Media Settings, Voice Settings Parameters

| Parameter | Description |
|---|---|
| Answer Detector Sensitivity [AnswerDetectorSensitivity] | Determines the Answer Detector sensitivity. The range is 0 (most sensitive) to 2 (least sensitive). The default is 0. |
| CAS Transport Type [CASTransportType] | <ul style="list-style-type: none">▪ [0] CAS Events Only = Disable CAS relay (default).▪ [1] CAS RFC2833 Relay = Enable CAS relay mode using RFC 2833. <p>The CAS relay mode can be used with the TDM tunneling feature to enable tunneling over IP for both voice and CAS signaling bearers.</p> |
| DTMF Generation Twist [DTMFGenerationTwist] | Defines a delta (in dB) between the high and low frequency components in the DTMF signal. Positive decibel values cause the higher frequency component to be stronger than the lower one. Negative values cause the opposite effect. For any parameter value, both components change so that their average is constant. The range is -10 to 10. The default value is 0. |

5.7.2 Configuring the Fax / Modem / CID Settings

The 'Fax / Modem / CID Settings' screen is used for configuring fax, modem, and Caller ID (CID) parameters.

➤ **To configure the Fax, Modem, and CID Settings parameters, take these 4 steps:**

1. Open the 'Fax / Modem / CID Settings' screen (**Advanced Configuration** menu > **Media Settings** > **Fax / Modem / CID Settings** option).

Figure 5-42: Fax / Modem / CID Settings Screen

| Fax/Modem/CID Settings | |
|-------------------------------------|---------------|
| Fax Transport Mode | T.38 Relay |
| Caller ID Transport Type | Mute |
| Caller ID Type | Bellcore |
| V.21 Modem Transport Type | Disable |
| V.22 Modem Transport Type | Enable Bypass |
| V.23 Modem Transport Type | Enable Bypass |
| V.32 Modem Transport Type | Enable Bypass |
| V.34 Modem Transport Type | Enable Bypass |
| Fax Relay Redundancy Depth | 0 |
| Fax Relay Enhanced Redundancy Depth | 4 |
| Fax Relay ECM Enable | Enable |
| Fax Relay Max Rate (bps) | 14400 |
| Fax/Modem Bypass Coder Type | G711Alaw |
| Fax/Modem Bypass Packing Factor | 1 |
| CNG Detector Mode | Disable |

2. Configure the Fax / Modem / CID Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-38: Media Settings -- Fax/Modem/CID Parameters

| Parameter | Description |
|--|---|
| Fax Transport Mode [FaxTransportMode] | <p>Fax Transport Mode that the gateway uses.</p> <ul style="list-style-type: none"> ▪ [0] Disable = transparent mode. ▪ [1] T.38 Relay = (default). ▪ [2] Bypass. ▪ [3] Events Only. <p>Note: If parameter IsFaxUsed = 1, then FaxTransportMode is always set to 1 (T.38 relay).</p> |
| Caller ID Transport Type [CallerIDTransportType] | <p>Defines the Caller ID Transport type.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable ▪ [1] Relay = Relay ▪ [3] Mute = Mute |
| Caller ID Type [CallerIDType] | <p>Defines one of the following standards for detection (FXO) and generation (FXS) of Caller ID, and detection (FXO) generation (FXS) of MWI (when specified) signals:</p> <ul style="list-style-type: none"> ▪ [0] Bellcore = Caller ID and MWI (default) ▪ [1] ETSI = Caller ID and MWI ▪ [2] NTT ▪ [4] Britain ▪ [16] DTMF ETSI ▪ [17] Denmark = Caller ID and MWI ▪ [18] India ▪ [19] Brazil <p>Notes:</p> <ul style="list-style-type: none"> ▪ Typically, the Caller ID signals are generated/detected between the first and second rings. However, sometimes the Caller ID is detected before the first ring signal (in such a scenario, configure RingsBeforeCallerID to 0). ▪ Caller ID detection for Britain [4] is not supported on the gateway's FXO ports. Only FXS ports can generate the Britain [4] Caller ID. ▪ To select the Bellcore Caller ID sub standard, use the parameter 'BellcoreCallerIDTypeOneSubStandard'. To select the ETSI Caller ID sub standard, use the parameter 'ETSICallerIDTypeOneSubStandard'. ▪ To select the Bellcore MWI sub standard, use the parameter 'BellcoreVMWITypeOneStandard'. To select the ETSI MWI sub standard, use the parameter 'ETSIVMWITypeOneStandard'. ▪ If you define NTT (i.e., 2) for the caller ID type, you need to define the NTT DID signaling form (FSK or DTMF) using NTTDIDSignallingForm. |

Table 5-38: Media Settings -- Fax/Modem/CID Parameters

| Parameter | Description |
|---|---|
| V.21 Modem Transport Type [V21ModemTransportType] | V.21 Modem Transport Type that the gateway uses. <ul style="list-style-type: none"> [0] Disable = Disable (Transparent) -- default [1] Enable Relay = N/A [2] Enable Bypass. [3] Events Only = Transparent with Events. |
| V.22 Modem Transport Type [V22ModemTransportType] | V.22 Modem Transport Type that the gateway uses. <ul style="list-style-type: none"> [0] Disable = Disable (Transparent) [1] Enable Relay = N/A [2] Enable Bypass = (default) [3] Events Only = Transparent with Events |
| V.23 Modem Transport Type [V23ModemTransportType] | V.23 Modem Transport Type that the gateway uses. <ul style="list-style-type: none"> [0] Disable = Disable (Transparent) [1] Enable Relay = N/A [2] Enable Bypass = (default) [3] Events Only = Transparent with Events |
| V.32 Modem Transport Type [V32ModemTransportType] | V.32 Modem Transport Type that the gateway uses. <ul style="list-style-type: none"> [0] Disable = Disable (Transparent) [1] Enable Relay = N/A [2] Enable Bypass = (default) [3] Events Only = Transparent with Events Note: This option applies to V.32 and V.32bis modems. |
| V.34 Modem Transport Type [V34ModemTransportType] | V.90 / V.34 Modem Transport Type that the gateway uses. <ul style="list-style-type: none"> [0] Disable = Disable (Transparent) [1] Enable Relay = N/A [2] Enable Bypass = (default) [3] Events Only = Transparent with Events |
| Fax Relay Redundancy Depth [FaxRelayRedundancyDepth] | Number of times that each fax relay payload is retransmitted to the network. This parameter is applicable only to non-V.21 packets. The valid range is 0 to 2, where 0 is no redundancy, 1 is one packet redundancy, and 2 is two packet redundancy. The default value is 0. |
| Fax Relay Enhanced Redundancy Depth [FaxRelayEnhancedRedundancyDepth] | Number of times that control packets are retransmitted when using the T.38 standard. The valid range is 0 to 4. The default value is 2. |
| Fax Relay ECM Enable [FaxRelayECMEnable] | <ul style="list-style-type: none"> [0] Disable = Error Correction Mode (ECM) mode is not used during fax relay. [1] Enable = ECM mode is used during fax relay (default). |

Table 5-38: Media Settings -- Fax/Modem/CID Parameters

| Parameter | Description |
|--|--|
| Fax Relay Max Rate (bps) [FaxRelayMaxRate] | <p>Maximum rate (in bps), at which fax relay messages are transmitted (outgoing calls).</p> <ul style="list-style-type: none"> ▪ [0] 2400 = 2.4 kbps. ▪ [1] 4800 = 4.8 kbps. ▪ [2] 7200 = 7.2 kbps. ▪ [3] 9600 = 9.6 kbps. ▪ [4] 12000 = 12.0 kbps. ▪ [5] 14400 = 14.4 kbps (default). <p>Note: The rate is negotiated between the sides, i.e., the gateway adapts to the capabilities of the remote side.</p> |
| Fax/Modem Bypass Coder Type [FaxModemBypassCoderType] | <p>Coder the gateway uses when performing fax/modem bypass. Usually, high-bit-rate coders such as G.711 should be used.</p> <ul style="list-style-type: none"> ▪ [0] G.711Alaw = G.711 A-law 64 (default). ▪ [1] G.711Mulaw = G.711 μ-law. |
| Fax/Modem Bypass Packing Factor [FaxModemBypassM] | <p>Number of (20 msec) coder payloads that are used to generate a fax/modem bypass packet. The valid range is 1, 2 or 3 coder payloads. The default value is 1 coder payload.</p> |
| CNG Detector Mode [CNGDetectorMode] | <ul style="list-style-type: none"> ▪ [0] Disable = The originating gateway doesn't detect CNG; the CNG signal passes transparently to the remote side (default). ▪ [1] Relay = CNG is detected on the originating side. CNG packets are sent to the remote side according to T.38 (if IsFaxUsed = 1) and the fax session is started. A Re-INVITE message isn't sent and the fax session starts by the terminating gateway. This option is useful (for example) when the originating gateway is located behind a firewall that blocks incoming T.38 packets on ports that have not yet received T.38 packets from the internal network (i.e., originating gateway). ▪ [2] Events Only = CNG is detected on the originating side. The CNG signal passes transparently to the remote side and a fax session is started by the originating side using Re-INVITE message. Usually, T.38 fax session starts when the 'preamble' signal is detected by the answering side. Some SIP gateways don't support the detection of this fax signal on the answering side, thus, for these cases it is possible to configure the gateway to start the T.38 fax session when the CNG tone is detected by the originating side. However, this mode is not recommended. |

5.7.3 Configuring the RTP / RTCP Settings

The 'RTP / RTCP Settings' screen is used for configuring RTP/RTCP parameters.

➤ **To configure the RTP / RTCP Settings parameters, take these 4 steps:**

1. Open the 'RTP / RTCP Settings' screen (**Advanced Configuration** menu > **Media Settings** > **RTP / RTCP Settings** option).

| RTP/RTCP Settings | |
|---|-----------------------|
| Dynamic Jitter Buffer Minimum Delay | 10 |
| Dynamic Jitter Buffer Optimization Factor | 10 |
| RTP Redundancy Depth | 0 |
| Packing Factor | 1 |
| Basic RTP Packet Interval | Default |
| RTP Directional Control | Transmit-Receive |
| RFC 2833 TX Payload Type | 96 |
| RFC 2833 RX Payload Type | 96 |
| RFC 2198 Payload Type | 104 |
| Fax Bypass Payload Type | 102 |
| Enable RFC 3389 CN Payload Type | Disable |
| Comfort Noise Generation Negotiation | Disable |
| Analog Signal Transport Type | Ignore analog signals |
| RTP Base UDP Port | 6000 |
| Remote RTP Base UDP Port | 0 |
| ! RTP Multiplexing Local UDP Port | 0 |
| ! RTP Multiplexing Remote UDP Port | 0 |
| RTCP XR Settings | |
| Enable RTCP XR | Disable |
| RTCP XR Report Mode | Disable |
| RTCP XR Packet Interval | 0 |
| Disable RTCP XR Interval Randomization | Disable |
| RTCP XR Collection Server | |

2. Configure the RTP / RTCP Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-39: Media Settings, RTP / RTCP Parameters

| Parameter | Description |
|--|--|
| Dynamic Jitter Buffer Minimum Delay [DJBufMinDelay] | Minimum delay for the Dynamic Jitter Buffer. The valid range is 0 to 150 milliseconds. The default delay is 10 milliseconds. Note: For more information on the Jitter Buffer, refer to 'Dynamic Jitter Buffer Operation' on page 397. |
| Dynamic Jitter Buffer Optimization Factor [DJBufOptFactor] | Dynamic Jitter Buffer frame error / delay optimization factor. The valid range is 0 to 13. The default factor is 10. Notes: <ul style="list-style-type: none"> Set to 13 for data (fax and modem) calls. For more information on the Jitter Buffer, refer to 'Dynamic Jitter Buffer Operation' on page 397. |
| RTP Redundancy Depth [RTPRedundancyDepth] | <ul style="list-style-type: none"> [0] 0 = Disable the generation of redundant packets (default). [1] 1 = Enable the generation of RFC 2198 redundancy packets. |
| Packing Factor [RTPPackingFactor] | N/A. Controlled internally by the gateway according to the selected coder. |
| Basic RTP Packet Interval [BasicRTPPacketInterval] | N/A. Controlled internally by the gateway according to the selected coder. Note: This parameter should not be used. Use the 'Coders' screen under 'Protocol Definition' instead. |
| RTP Directional Control [RTPDirectionControl] | N/A. Controlled internally by the gateway according to the selected coder. |
| RFC 2833 TX Payload Type [RFC2833TxPayloadType] | N/A. Use the <i>ini</i> file parameter RFC2833PayloadType instead. |
| RFC 2833 RX Payload Type [RFC2833RxPayloadType] | N/A. Use the <i>ini</i> file parameter RFC2833PayloadType instead. |
| RFC 2198 Payload Type [RFC2198PayloadType] | RTP redundancy packet payload type, according to RFC 2198. The range is 96-127. The default is 104. Applicable if RTP Redundancy Depth = 1. |
| Fax Bypass Payload Type [FaxBypassPayloadType] | Determines the fax bypass RTP dynamic payload type. The valid range is 96 to 120. The default value is 102. |
| Enable RFC 3389 CN Payload Type [EnableStandardSIDPayloadType] | Determines whether Silence Indicator (SID) packets that are sent and received are according to RFC 3389. <ul style="list-style-type: none"> [0] Disable = G.711 SID packets are sent in a proprietary method (default). [1] Enable = SID (comfort noise) packets are sent with the RTP SID payload type according to RFC 3389. Applicable to G.711 and G.726 coders. |

Table 5-39: Media Settings, RTP / RTCP Parameters

| Parameter | Description |
|---|--|
| Comfort Noise Generation Negotiation [ComfortNoiseNegotiation] | <p>Enables negotiation and usage of Comfort Noise (CN).</p> <ul style="list-style-type: none"> [0] Disable = Disable (default). [1] Enable = Enable Comfort Noise negotiation <p>The use of CN is indicated by including a payload type for CN on the media description line of the SDP. The gateway can use CN with a codec whose RTP timestamp clock rate is 8,000 Hz (G.711/G.726). The static payload type 13 is used. The use of CN is negotiated between sides; therefore, if the remote side doesn't support CN, it is not used.</p> <p>Note: Silence Suppression must be enabled to generate CN.</p> |
| Analog Signal Transport Type [AnalogSignalTransportType] | <p>Determines the analog signal transport type.</p> <ul style="list-style-type: none"> [0] Ignore Analog Signals = Ignore (default) [1] RFC2833 Analog Signal Relay = Transfer hookflash via RFC 2833 |
| RTP Base UDP Port [BaseUDPPort] | <p>Lower boundary of UDP port used for RTP, RTCP (Real-Time Control Protocol) (RTP port + 1) and T.38 (RTP port + 2). The upper boundary is the Base UDP Port + 10 * (number of gateway's channels).</p> <p>The range of possible UDP ports is 6,000 to 64,000. The default base UDP port is 6000.</p> <p>For example: If the Base UDP Port is set to 6000 (the default) then:</p> <p>1) The first channel uses the following ports: RTP 6000, RTCP 6001 and T.38 6002, 2) the second channel uses: RTP 6010, RTCP 6011 and T.38 6012, etc.</p> <p>Note: If RTP Base UDP Port is not a factor of 10, the following message is generated: 'invalid local RTP port'.</p> <p>For detailed information on the default RTP/RTCP/T.38 port allocation, refer to the <i>SIP Series Reference Manual</i>.</p> |
| Remote RTP Base UDP Port [RemoteBaseUDPPort] | <p>Determines the lower boundary of UDP ports used for RTP, RTCP and T.38 by a remote gateway. If this parameter is set to a non-zero value, ThroughPacket™ is enabled. Note that the value of RemoteBaseUDPPort on the local gateway must equal the value of BaseUDPPort of the remote gateway. The gateway uses these parameters to identify and distribute the payloads from the received multiplexed IP packet to the relevant channels.</p> <p>The valid range is the range of possible UDP ports: 6,000 to 64,000.</p> <p>The default value is 0 (ThroughPacket is disabled).</p> <p>For detailed information on ThroughPacket, refer to 'RTP Multiplexing (ThroughPacket)' on page 396.</p> <p>Notes:</p> <ul style="list-style-type: none"> To enable ThroughPacket the parameters L1L1ComplexTxUDPPort and L1L1ComplexRxUDPPort must be set to a non-zero value. When VLANs are implemented, the ThroughPacket mechanism is not supported. |

Table 5-39: Media Settings, RTP / RTCP Parameters

| Parameter | Description |
|--|---|
| RTP Multiplexing Local UDP Port [L1L1ComplexTxUDPPort] | Determines the local UDP port used for outgoing multiplexed RTP packets (applies to the ThroughPacket™ mechanism). The valid range is the range of possible UDP ports: 6,000 to 64,000. The default value is 0 (ThroughPacket is disabled). This parameter cannot be changed on-the-fly and requires a gateway reset. |
| RTP Multiplexing Remote UDP Port [L1L1ComplexRxUDPPort] | Determines the remote UDP port the multiplexed RTP packets are sent to, and the local UDP port used for incoming multiplexed RTP packets (applies to the ThroughPacket™ mechanism). The valid range is the range of possible UDP ports: 6,000 to 64,000. The default value is 0 (ThroughPacket is disabled). This parameter cannot be changed on-the-fly and requires a gateway reset. Note: All gateways that participate in the same ThroughPacket session must use the same L1L1ComplexRxUDPPort. |
| RTCP XR Settings (For a detailed description of RTCP-XR reports, refer to the SIP Series Reference Manual) | |
| Enable RTCP XR [VQMonEnable] | Enables voice quality monitoring and RTCP Extended Reports (RTCP-XR). <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default) ▪ [1] Enable = Enables |
| RTCP XR Report Mode [RTCPXRReportMode] | Determines whether or not RTCP-XR reports are sent to the Event State Compositor (ESC) and if so, defines the interval in which they are sent. <ul style="list-style-type: none"> ▪ [0] Disable = RTCP-XR reports are not sent to the ESC (default) ▪ [1] End Call = RTCP-XR reports are sent to the ESC at the end of each call. ▪ [2] End Call & Periodic = RTCP-XR reports are sent to the ESC at the end of each call and periodically according to the parameter RTCPInterval. |
| RTCP XR Packet Interval [RTCPInterval] | Defines the time interval (in msec) between adjacent RTCP reports. The interval range is 0 to 65,535. The default interval is 5,000. |
| Disable RTCP XR Interval Randomization [DisableRTCPRandomize] | Controls whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter RTCPInterval. <ul style="list-style-type: none"> ▪ [0] Disable = Randomize (default) ▪ [1] Enable = No Randomize |
| RTCP XR Collection Server [RTCPXREscIP] | IP address of the Event State Compositor (ESC). The gateway sends RTCP-XR reports using PUBLISH messages to this server. The address can be configured as a numerical IP address or as a domain name. |

5.7.4 Configuring the IPmedia Settings

The 'IPmedia Settings' screen is used for configuring the IPmedia server parameters.

➤ **To configure the IPmedia parameters, take these 4 steps:**

1. Open the 'IPmedia Parameters' screen (**Advanced Configuration** menu > **Media Settings** > **IPmedia Settings** option).

Figure 5-43: IPmedia Settings Screen

| IPmedia Settings | |
|-------------------------------------|-----------|
| Enable Answer Detector | Disable ▼ |
| Answer Detector Activity Delay | 0 |
| Answer Detector Silence Time | 10 |
| Answer Detector Redirection | Disable ▼ |
| Answer Detector Sensitivity | 0 ▼ |
| Answer machine detector sensitivity | 3 |
| Enable AGC | Disable ▼ |
| AGC Slope | 3 |
| AGC Redirection | 0 ▼ |
| AGC Target Energy | 19 |
| Enable Energy Detector | Disable ▼ |
| Energy Detector Quality Factor | 4 |
| Energy Detector Threshold | 3 |
| Enable Pattern Detector | Disable ▼ |
| Active Speakers Min Interval | 20 |
| | 60 |

2. Configure the media server parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-40: Media Server Parameters

| Parameter | Description |
|--|--|
| Enable Answer Detector [EnableAnswerDetector] | N/A. |
| Answer Detector Activity Delay [AnswerDetectorActivityDelay] | N/A. |
| Answer Detector Silence Time [AnswerDetectorSilenceTime] | N/A. |
| Answer Detector Redirection [AnswerDetectorRedirection] | N/A. |
| Answer Detector Sensitivity [AnswerDetectorSensitivity] | Determines the Answer Detector sensitivity. The range is 0 (most sensitive) to 2 (least sensitive). The default is 0. |
| Enable Energy Detector [EnableEnergyDetector] | N/A |
| Energy Detector Quality Factor [EnergyDetectorQualityFactor] | N/A |
| Energy Detector Threshold [EnergyDetectorThreshold] | N/A |
| Enable Pattern Detector [EnablePatternDetector] | Enables or disables the activation of the Pattern Detector (PD). Valid options include: <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default) ▪ [1] Enable = Enable |

5.7.5 Configuring the Hook-Flash Settings

The 'Hook-Flash Settings' screen is used for configuring Hook-Flash parameters.

➤ **To configure the Hook-Flash Settings parameters, take these 4 steps:**

1. Open the 'Hook-Flash Settings' screen (**Advanced Configuration** menu > **Media Settings** > **Hook-Flash Settings** option).

Figure 5-44: Hook-Flash Settings Screen

| Hook-Flash Settings | |
|---|-----|
| Min. Hook-Flash Detection Period [msec] | 300 |
| Max. Hook-Flash Detection Period [msec] | 700 |

2. Configure the Hook-Flash Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-41: Media Settings, Hook-Flash Settings Parameters

| Parameter | Description |
|--|---|
| Min. Flash-Hook Detection Period [msec] [MinFlashHookTime] | <p>Sets the minimal time (in msec) for detection of a flash-hook event (for FXS only). The valid range is 25 to 300. The default value is 300 msec. Detection is guaranteed for flash hook periods of at least 60 msec (when setting the minimal time to 25). Flash-hook signals that last a shorter period of time are ignored.</p> <p>Note: It's recommended to reduce the detection time by 50 msec from the desired value (e.g. if you set the value to 200 msec, then enter 150 msec (i.e. 200 minus 50).</p> |
| Max. Flash-Hook Detection Period [msec] [FlashHookPeriod] | <p>Defines the flash-hook period (in msec) for both analog and IP sides. For the analog side it defines the following:</p> <ul style="list-style-type: none"> ▪ Maximal hook-flash detection period (for FXS modules). A longer signal is considered offhook / onhook event. ▪ Hook-flash generation period (for FXO modules). <p>For the IP side it defines the flash-hook period that is reported to IP. The valid range is 25 to 1500. The default value is 700 msec.</p> <p>Note: For FXO modules, a constant of 100 msec must be added to the required hook-flash period. For example, to generate a 450 msec hook-flash, set FlashHookPeriod to 550.</p> |

5.7.6 Configuring the General Media Settings

- To configure the General Media Settings parameters, take these 4 steps:

1. Open the 'General Media Settings' screen (**Advanced Configuration** menu > **Media Settings** > **General Media Settings** option).

Figure 5-45: General Media Settings Screen

| General Media Settings | |
|-------------------------------|--|
| ! DSP Version Template Number | <input type="text" value="0"/> |
| ! Max Echo Canceller Length | Default <input type="button" value="v"/> |
| ! Enable Continuity Tones | Disable <input type="button" value="v"/> |

2. Configure the General Media Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-42: Media Settings - General Media Settings Parameters

| Parameter | Description |
|---|--|
| Max Echo Canceller Length [MaxEchoCancellerLength] | <p>Maximum Echo Canceller Length in msec:</p> <ul style="list-style-type: none"> ▪ [0] Default = based on various internal gateway settings to attain maximum channel capacity (default) ▪ [11] 64 = 64 msec ▪ [22] 128 = 128 msec <p>Notes:</p> <ul style="list-style-type: none"> ▪ Using 28 msec reduces the channel capacity to 200 channels. ▪ The gateway must be reset after the value of MaxEchoCancellerLength is changed. ▪ It isn't necessary to configure the parameter EchoCancellerLength as it automatically acquires its value from the parameter MaxEchoCancellerLength. |
| Enable Continuity Tones | N/A. |

5.8 PSTN Settings

5.8.1 Configuring the PSTN Settings

The **PSTN Settings** submenu allows you to configure various PSTN settings.

5.8.1.1 Trunk Settings

The 'Trunk Settings' screen enables you to configure the gateway's E1/T1 trunks. For configuring the trunks using the *ini* file parameters, refer to 'PSTN Parameters' on page 340.

➤ **To configure the Trunk Settings, take these 9 steps:**

1. Open the 'Trunk Settings' screen (**Advanced Configuration** menu > **PSTN Settings** > **Trunk Settings**).

Figure 5-46: Trunk Settings Screen

| Trunk Number | 1 | 2 | 3 | 4 |
|--------------|---|---|---|---|
| Trunk Status | | | | |

| Trunk Settings | |
|---------------------------------|----------------------|
| Trunk Configuration | |
| Module ID | 1 |
| Trunk ID | 4 |
| Trunk Configuration State | Active |
| Protocol Type | E1 EURO ISDN |
| Clock Master | Recovered |
| Auto Clock Trunk Priority | 0 |
| Line Code | HDB3 |
| Line Build Out Loss | 0 dB |
| Trace Level | No Trace |
| Line Build Out Overwrite | OFF |
| Framing Method | Extended Super Frame |
| ISDN Configuration | |
| ISDN Termination Side | User side |
| Q931 Layer Response Behavior | 0x0 --> |
| Outgoing Calls Behavior | 0x400 --> |
| Incoming Calls Behavior | 0x0 --> |
| General Call Control Behavior | 0x0 --> |
| NFAS Group Number | 0 |
| IUA Interface ID | -1 |
| NFAS Interface ID | 255 |
| D-channel Configuration | PRIMARY |
| PSTN Settings | |
| PSTN Alert Timeout | 180 |
| Enable ECT | Disable |
| Play Ringback Tone to Trunk | Not Configured |
| Local ISDN Ringback Tone Source | PBX |

Initially, the screen appears with the parameter fields grayed (indicating read-only), and the **Stop Trunk** button is displayed at the bottom of the screen (indicating that the trunk is currently active).

The Trunk Status icons display the current status of the trunk:

- Grey: disabled
 - Green: active
 - Yellow: RAI alarm
 - Red: LOS / LOF alarm
 - Blue: AIS alarm
 - Orange: D-channel alarm (ISDN only)
2. Select the trunk you want to configure, by clicking the Trunk Status icon pertaining to the trunk. The read-only 'Trunk ID' field displays the trunk number that you selected. The parameters displayed in the screen pertain to the selected trunk only.
 3. Click the **Stop Trunk** button (unless modifying a Dial Plan -- refer to note below); the trunk is stopped. This is indicated by the following:
 - The 'Trunk Configuration State' read-only field displays 'Inactive'.
 - The **Stop Trunk** button is replaced by the **Apply Trunk Settings** button. (When all trunks are stopped, the **Apply to all Trunks** button also appears.)
 - The parameters are no longer grayed and can now be modified.



Notes:

- When CAS is selected as the Protocol Type (refer to Step 4 below), you can apply a dial plan (in the 'Dial plan' field) without stopping the trunk. Modifying the Dial Plan causes the button located at the bottom of the screen to become **Apply Dial Plan**.
- If the trunk protocol type is CAS (displayed in the 'Protocol Type' field), you can apply or modify a dial plan (in the 'Dial Plan' field) without stopping the trunk. Modifying the dial plan replaces the **Stop Trunk** with the **Apply Dial Plan** button.
- If the trunk can't be stopped because it provides the gateway's clock (assuming the gateway is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the gateway's clock or enable 'TDM Bus PSTN Auto Clock' in the 'TDM Bus Settings' screen. To assign a different E1/T1 trunk that provides the gateway's clock, access the 'TDM Bus Setting' screen ('Configuring the TDM Bus Settings' on page 221) and change the 'TDM Bus Local Reference' number to any other trunk number (this operation can be performed on-the-fly).

4. From the 'Protocol Type' drop-down list, select the required protocol.


Notes:

- Different trunks can be defined with different protocols (CAS or ISDN variants) on the same gateway (subject to the constraints in the gateway's Release Notes).
- When modifying the 'Protocol Type' field, the menu is automatically updated according to the selected protocol (ISDN, CAS, or Transparent). Additional parameters are appropriate to the selected protocol type.

5. Modify the relevant trunk configuration parameters according to your requirements.
6. To configure the different behavior bits: either enter the exact hexadecimal value of the bits in the field to the right of the relevant behavior parameter, or directly configure each bit field by completing the following steps:
 - a. Click the arrow button (-->) to the right of the relevant behavior parameter; a new window appears.
 - b. Modify each bit field according to your requirements.
 - c. Click the **Submit** button to save your changes.
7. After modifying the parameters:
 - To apply the changes to the selected trunk only, click the **Apply Trunk Settings** button.
 - To apply the changes to all the trunks, click the **Apply to all Trunks** button.
8. The screen is refreshed; parameters become read-only (indicated by being grayed). The **Stop Trunk** button replaces the **Apply Trunk Settings** button.
9. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.



Note: Some parameter configuration options require device reset; when this is the case, the Embedded Web Server prompts the user.

10. To reset the gateway, refer to 'Resetting the Gateway' on page 279.

Table 5-43: E1/T1/J1 Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| Protocol Type [ProtocolType] | <p>Sets the PSTN protocol to be used for this trunk.</p> <ul style="list-style-type: none"> ▪ [1] E1 EURO ISDN ▪ [2] T1 CAS ▪ [3] T1 RAW CAS ▪ [4] T1 TRANSPARENT ▪ [5] E1 TRANSPARENT 31 ▪ [6] E1 TRANSPARENT 30 ▪ [7] E1 MFCR2 ▪ [8] E1 CAS ▪ [9] E1 RAW CAS ▪ [10] T1 NI2 ISDN ▪ [11] T1 4ESS ISDN ▪ [12] T1 5ESS 9 ISDN ▪ [13] T1 5ESS 10 ISDN ▪ [14] T1 DMS100 ISDN ▪ [15] J1 TRANSPARENT ▪ [16] T1 NTT ISDN = Japan - Nippon Telegraph ▪ [17] E1 AUSTEL ISDN = Australian Telecom ▪ [18] T1 HKT ISDN = Hong Kong - HKT ▪ [19] E1 KOR ISDN = Korean operator ▪ [20] T1 HKT ISDN = Hong Kong - HKT over T1 ▪ [21] E1 QSIG ▪ [23] T1 QSIG ▪ [31] E1 FRENCH VN3 ISDN ▪ [35] T1 DMS100 Meridian ISDN ▪ [40] E1 NI2 ISDN ▪ [41] E1 CAS R15 <p>Note: The gateway simultaneously supports different variants of CAS and PRI protocols on different E1/T1 spans (no more than four simultaneous PRI variants).</p> |
| Clock Master [ClockMaster] | <p>Determines the Tx clock source of the E1/T1 line.</p> <ul style="list-style-type: none"> ▪ [0] Recovered = Generate the clock according to the Rx of the E1/T1 line (default). ▪ [1] Generated = Generate the clock according to the internal TDM bus. <p>For detailed information on configuring the gateway's clock settings, refer to 'Clock Settings' on page 439.</p> <p>Note: The source of the internal TDM bus clock is determined by the parameter TDMBusClockSource.</p> |

Table 5-43: E1/T1/J1 Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| Auto Clock Trunk Priority [AutoClockTrunkPriority] | <p>Defines the trunk priority for auto-clock fallback (per trunk parameter).</p> <ul style="list-style-type: none"> 0 to 99 = priority (0 is the highest = default). 100 = the SW never performs a fallback to that trunk (usually used to mark un-trusted source of clock). <p>Note: Fallback is enabled when the TDMBusPSTNAutoClockEnable parameter is set to 1.</p> |
| Line Code [LineCode] | <p>Use to select B8ZS or AMI for T1 spans, and HDB3 or AMI for E1 spans.</p> <ul style="list-style-type: none"> [0] B8ZS = use B8ZS line code (for T1 trunks only) default. [1] AMI = use AMI line code. [2] HDB3 = use HDB3 line code (for E1 trunks only). |
| Line Build Out Loss [LineBuildOut.Loss] | <p>Selects the line build out loss to be used for T1 trunks.</p> <ul style="list-style-type: none"> [0] 0 dB (default) [1] -7.5 dB [2] -15 dB [3] -22.5 dB <p>Note: This parameter is not applicable for E1 trunks.</p> |
| Trace Level [TraceLevel] | <p>Defines the trace level:</p> <ul style="list-style-type: none"> [0] No Trace (default) [1] Full ISDN Trace [2] Layer 3 ISDN Trace [3] Only ISDN Q.931 Messages Trace [4] Layer 3 ISDN No Duplication Trace |
| Framing Method [FramingMethod] | <p>Selects the physical framing method used for the trunk.</p> <ul style="list-style-type: none"> [0] = default according to protocol type E1 or T1. E1 default = E1 CRC4 MultiFrame Format extended G.706B (as c); T1 default = T1 Extended SuperFrame with CRC6 (as D). [1] = T1 SuperFrame Format (as B). [a] = E1 DoubleFrame Format [b] = E1 CRC4 MultiFrame Format [c] = E1 CRC4 MultiFrame Format extended G.706B [A] = T1 4-Frame multiframe. [B] = T1 12-Frame multiframe (D4). [C] = T1 Extended SuperFrame without CRC6 [D] = T1 Extended SuperFrame with CRC6 [E] = T1 72-Frame multiframe (SLC96) [F] = J1 Extended SuperFrame with CRC6 (Japan) |

Table 5-43: E1/T1/J1 Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|---|
| ISDN Configuration Parameters | |
| ISDN Termination Side [TerminationSide] | <p>Selects the ISDN termination side. Applicable only to ISDN protocols.</p> <ul style="list-style-type: none"> [0] User side = ISDN User Termination Side (TE) (default) [1] Network side = ISDN Network Termination Side (NT) <p>Note: select 'User side' when the PSTN or PBX side is configured as 'Network side', and vice-versa. If you don't know the gateway ISDN termination side, choose 'User side' and refer to the 'Status & Diagnostics > Channel Status' screen. If the D-channel alarm is indicated, choose 'Network Side'.</p> |
| NFAS Group Number [NFASGroupNumber_x] | <p>Indicates the NFAS group number (NFAS member) for the selected trunk. 'x' identifies the Trunk ID.</p> <ul style="list-style-type: none"> 0 = Non NFAS trunk (default) 1 to 4 = NFAS group number <p>Trunks that belong to the same NFAS group have the same number. With ISDN Non-Facility Associated Signaling you can use single D-channel to control multiple PRI interfaces. Applicable only to T1 ISDN protocols.</p> |
| NFAS Interface ID [ISDNNFASInterfaceID_x] | <p>Defines a different Interface ID for each T1 trunk. The valid range is 0 to 100. The default interface ID equals to the trunk's ID. 'x' identifies the trunk ID.</p> <p>Note: To set the NFAS interface ID, configure ISDNIBehavior_x to include '512' feature per T1 trunk.</p> |
| D-channel Configuration [DChConfig_x] | <p>Defines primary, backup (optional), and B-channels only trunks. 'x' identifies the Trunk ID.</p> <ul style="list-style-type: none"> [0] PRIMARY= Primary Trunk (default) [1] BACKUP = Backup Trunk [2] NFAS = NFAS Trunk <p>Primary trunk contains D-channel that is used for signaling. Backup trunk contains backup D-channel that is used if the primary D-channel fails. The other NFAS trunks contain only 24 B-channels, without a signaling D-channel.</p> <p>Note: Applicable only to T1 ISDN protocols.</p> |

Table 5-43: E1/T1/J1 Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|--|
| Enable Receiving of Overlap Dialing [ISDNRxOverlap_x] | <p>Enable / disable Rx ISDN overlap per trunk ID.</p> <ul style="list-style-type: none"> [0] Disable = Disabled (default). [1] Enable = Enabled. <p>Notes:</p> <ul style="list-style-type: none"> If enabled, the gateway receives ISDN called number that is sent in the 'Overlap' mode. The SETUP message to IP is sent only after the number (including the 'Sending Complete' Info Element) was fully received (via SETUP and/or subsequent INFO Q.931 messages). The 'MaxDigits' parameter can be used to limit the length of the collected number for gateway ISDN overlap dialing (if sending complete is not received). If a digit map pattern is defined (DigitMapping), the gateway collects digits until a match is found (e.g., for closed numbering schemes) or until a timer expires (e.g., for open numbering schemes). If a match is found (or the timer expires), the digit collection process is terminated even if Sending Complete wasn't received. |
| Local ISDN Ringback Tone Source [LocalISDNRBSource_ID] | <p>Determines whether Ringback tone is played to the ISDN by the PBX / PSTN or by the gateway, where <i>ID</i> is the Trunk number (0-0-73).</p> <ul style="list-style-type: none"> [0] PBX = PBX / PSTN (default). [1] Gateway. <p>This parameter is applicable to ISDN protocols. It is used simultaneously with the parameter 'PlayRBTone2Trunk'.</p> |
| Progress Indicator to ISDN [ProgressIndicator2ISDN_ID] | <p>Progress indicator (PI) to ISDN, where <i>ID</i> is the Trunk number (0-3).</p> <ul style="list-style-type: none"> [-1] Not Configured = The PI in ISDN messages is set according to the 'Play Ringback to Tel' parameter (default). [0] No PI = PI is not sent to ISDN. [1] PI = 1; [8] PI = 8: The PI value is sent to PSTN in Q.931/Proceeding and Alerting messages. Typically, the PSTN/PBX cuts through the audio channel without playing local Ringback tone, enabling the originating party to hear remote Call Progress Tones or network announcements. |
| Set PI in Rx Disconnect Message [PIForDisconnectMsg_ID] | <p>Defines the gateway's behavior when a Disconnect message is received from the ISDN before a Connect message is received. Where <i>ID</i> is the Trunk number (0-3).</p> <ul style="list-style-type: none"> [-1] Not Configured = Sends a 183 message according to the received progress indicator (PI) in the ISDN Disconnect message. If PI = 1 or 8, the gateway sends a 183 response, enabling the PSTN to play a voice announcement to the IP side. If there isn't a PI in the Disconnect message, the call is released (default). [0] No PI = Don't send a 183 message to IP. The call is released. [1] PI = 1; [8] PI = 8: Sends a 183 message to IP. |

Table 5-43: E1/T1/J1 Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| ISDN Transfer Capabilities [ISDNTransferCapability_ID] | <p>Defines the IP-to-ISDN Transfer Capability of the Bearer Capability IE in ISDN Setup messages. ID is the Trunk number.</p> <ul style="list-style-type: none"> ▪ [0] Audio 3.1 = Audio (default). ▪ [1] Speech = Speech. ▪ [2] Data = Data. ▪ Audio 7 = Currently not supported. ▪ [-1] Not Configured <p>Note: If this parameter isn't configured or equals to '-1', Audio 3.1 capability is used.</p> |
| ISDN Flexible Behavior Parameters ISDN protocol is implemented in different Switches / PBXs by different vendors. Several implementations vary a little from the specification. Therefore, to provide a flexible interface that supports these ISDN variants, the ISDN behavior parameters are used. | |
| Q.931 Layer Response Behavior [ISDNIBehavior] | <p>Bit-field used to determine several behavior options that influence the behaviour of the Q.931 protocol. To select the options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable).</p> <ul style="list-style-type: none"> ▪ [1] NO STATUS ON UNKNOWN IE = Q.931 Status message isn't sent if Q.931 received message contains an unknown/unrecognized IE(s). By default, the Status message is sent. This parameter applies only to PRI variants in which sending of Status message is optional. ▪ [2] NO STATUS ON INV OP IE = Q.931 Status message isn't sent if an optional IE with invalid content is received. By default, the Status message is sent. This parameter applies only to PRI variants in which sending of Status message is optional. ▪ [4] ACCEPT UNKNOWN FAC IE = Accepts unknown/unrecognized Facility IE. Otherwise, the Q.931 message that contains the unknown Facility IE is rejected (default). This parameter applies to PRI variants where a complete ASN1 decoding is performed on Facility IE. ▪ [128] SEND USER CONNECT ACK = Connect ACK message is sent in response to received Q.931 Connect. Applicable only to Euro ISDN User side outgoing calls. Otherwise, the Connect ACK is not sent (default). ▪ [512] EXPLICIT INTERFACE ID = Enables to configure T1 NFAS Interface ID (refer to the parameter ISDNNFASInterfaceID_x). Applicable to 4/5ESS, DMS, NI-2 and HKT variants. ▪ [2048] ALWAYS EXPLICIT = Always set the Channel Identification IE to explicit Interface ID, even if the B-channel is on the same trunk as the D-channel. Applicable to 4/5ESS, DMS and NI-2 variants. ▪ [32768] ACCEPT MU LAW =Mu-Law is also accepted in ETSI. ▪ [65536] EXPLICIT PRES SCREENING = The calling party number (octet 3a) is always present even when presentation and |

Table 5-43: E1/T1/J1 Configuration Parameters

| ini File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| | <p>screening are at their default. Applicable to ETSI, NI-2 and 5ESS.</p> <ul style="list-style-type: none"> ▪ [131072] STATUS INCOMPATIBLE STATE = Clears the call on receipt of Q.931 Status with incompatible state. Otherwise, no action is taken (default). ▪ [262144] STATUS ERROR CAUSE = Clear call on receipt of STATUS according to cause value. ▪ [524288] ACCEPT A LAW =A-Law is also accepted in 5ESS. ▪ [2097152] RESTART INDICATION =acEV_PSTN_RESTART_CONFIRM is generated on receipt of a RESTART message. ▪ [4194304] FORCED RESTART =On data link (re)initialization, send RESTART if there is no call. ▪ [2147483648] NS 5ESS NATIONAL = Use the National mode of AT&T 5ESS for B-channel maintenance. <p>Note: To configure the gateway to support several ISDNBehavior features, add the individual feature values. For example, to support both [512] and [2048] features, set ISDNBehavior = 2560 (i.e., 512 + 2048).</p> |
| Outgoing Calls Behavior [ISDNOutCallsBehavior] | <p>This parameter determines several behaviour options that influence the behaviour of the ISDN Stack outgoing calls. To select options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable).</p> <ul style="list-style-type: none"> ▪ [2] USER SENDING COMPLETE =When this bit is set, the gateway doesn't automatically generate the information element 'Sending-complete' in the SETUP message. If this bit is not set, the gateway generates it automatically in the SETUP message only. ▪ [16] USE MU LAW = When set, the gateway sends G.711-m-Law in outgoing voice calls. When disabled, the gateway sends G.711-A-Law in outgoing voice calls. (Applicable only to the Korean variant.) ▪ [128] DIAL WITH KEYPAD = When enabled, the gateway uses the KEYPAD IE to store the called number digits instead of the CALLED_NB IE. (Only applicable to the KOR variant (Korean network). Useful for Korean switches that don't accept the CALLED_NB IE.) ▪ [256] STORE CHAN ID IN SETUP =When this bit is set, the gateway forces the sending of a Channel-id IE in an outgoing SETUP message even if it's not required by the standard (i.e., optional), and no Channel-id has been specified in the establishment request. This is useful for improving required compatibility with switches. On BRI lines, the Channel-id IE indicates 'any channel'. On PRI lines, it indicates an unused channel ID, preferred only. ▪ [572] USE A LAW = When set, the gateway sends G.711 A-Law in outgoing voice calls. When disabled, the gateway sends the default G.711-Law in outgoing voice calls. Applicable to E10 variant. |

Table 5-43: E1/T1/J1 Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|--|
| | <ul style="list-style-type: none"> ▪ [1024] = Numbering plan / type for T1 IP-to-Tel calling numbers are defined according to the manipulation tables or according to the RPID header (default). Otherwise, the plan / type for T1 calls are set according to the length of the calling number. ▪ [2048] = When this bit is set, the gateway accepts any IA5 character in the called_nb and calling_nb strings, and isn't restricted to extended digits only (i.e., 0-9,*,#). ▪ [16384] DLCI REVERSED OPTION = Behavior bit used in the IUA interface groups to indicate that the reversed format of the DLCI field must be used. <p>Note: When using the <i>ini</i> file to configure the gateway to support several ISDNOutCallsBehavior features, add the individual feature values. For example, to support both [2] and [16] features, set ISDNOutCallsBehavior = 18 (i.e., 2 + 16).</p> |
| Incoming Calls Behavior [ISDNInCallsBehavior] | <p>This is the bit-field used to determine several behavior options that influence how the ISDN Stack INCOMING calls behave. To select the options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable).</p> <ul style="list-style-type: none"> ▪ [32] DATA CONN RS = Sends a CONNECT (answer) message on NOT incoming Tel calls. ▪ [64] VOICE CONN RS = gateway sends a CONNECT (answer) message on incoming Tel calls. ▪ [2048] CHAN ID IN FIRST RS = Sends Channel ID in the first response to an incoming Q.931 Call Setup message. Otherwise, the Channel ID is sent only if the gateway requires changing the proposed Channel ID (default). ▪ [8192] CHAN ID IN CALL PROC = Sends Channel ID in a Q.931 Call Proceeding message. ▪ [65536] PROGR IND IN SETUP ACK = Includes Progress Indicator (PI=8) in Setup ACK message if an empty called number is received in an incoming Setup message. Applicable to overlap dialing mode. The parameter also directs the gateway to play a dial tone (for TimeForDialTone), until the next called number digits are received. ▪ [262144] = NI-2 second redirect number. You can select and use (in INVITE messages) the NI-2 second redirect number if two redirect numbers are received in Q.931 Setup for incoming Tel-to-IP calls. <p>Note: When using the <i>ini</i> file to configure the gateway to support several ISDNInCallsBehavior features, add the individual feature values. For example, to support both [2048] and [65536] features, set ISDNInCallsBehavior = 67584 (i.e., 2048 + 65536).</p> |

Table 5-43: E1/T1/J1 Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|---|
| General Call Control Behavior [ISDNGeneralCCBehavior] | <p>Bit-field used to determine several general CC behavior options. To select the options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable).</p> <ul style="list-style-type: none"> ▪ [2] = data calls with interworking indication use 64 kbps B-channels (physical only). ▪ [8] REVERSE CHAN ALLOC ALGO = Channel ID allocation algorithm. ▪ [16] = The gateway clears down the call if it receives a NOTIFY message specifying 'User-Suspended'. A NOTIFY (User-Suspended) message is used by some networks (e.g., in Italy or Denmark) to indicate that the remote user has cleared the call, especially in the case of a long distance voice call. ▪ [32] CHAN ID 16 ALLOWED = Applies only to ETSI E1 lines (30B+D). Enables handling the differences between the newer QSIG standard (ETS 300-172) and other ETSI-based standards (ETS 300-102 and ETS 300-403) in the conversion of B-channel ID values into timeslot values: <ul style="list-style-type: none"> 1) In 'regular ETSI' standards, the timeslot is identical to the B-channel ID value, and the range for both is 1 to 15 and 17 to 31. The D-channel is identified as channel-id #16 and carried into the timeslot #16. 2) In newer QSIG standards, the channel-id range is 1 to 30, but the timeslot range is still 1 to 15 and 17 to 31. The D-channel is not identified as channel-id #16, but is still carried into the timeslot #16. When this bit is set, the channel ID #16 is considered as a valid B-channel ID, but timeslot values are converted to reflect the range 1 to 15 and 17 to 31. This is the new QSIG mode of operation. When this bit is not set (default), the channel_id #16 is not allowed, as for all ETSI-like standards. ▪ [64] USE T1 PRI = PRI interface type is forced to T1. ▪ [128] USE E1 PRI = PRI interface type is forced to E1. ▪ [256] START WITH B CHAN OOS = B-channels start in the Out-Of-Service state (OOS). ▪ [512] CHAN ALLOC LOWEST = CC allocates B-channels starting from the lowest available B-channel id. ▪ [1024] CHAN ALLOC HIGHEST = CC allocates B-channels starting from the highest available B-channel id. <p>Note: When using the <i>ini</i> file to configure the gateway to support several ISDNGeneralCCBehavior features, add the individual feature values. For example, to support both [16] and [32] features, set ISDNGeneralCCBehavior = 48 (i.e., 16 + 32).</p> |

Table 5-43: E1/T1/J1 Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| CAS Configuration | |
| CAS Table [CASTableIndex_x] | <p>Defines CAS protocol for each trunk ID from a list of CAS protocols defined by the parameter CASFileName_Y.</p> <p>For example: CASFileName_0 = 'E_M_WinkTable.dat' CASFileName_1 = 'E_M_ImmediateTable.dat' CASTableIndex_0 = 0 CASTableIndex_1 = 0 CASTableIndex_2 = 1 CASTableIndex_3 = 1</p> <p>Trunks 0 and 1 use the E&M Winkstart CAS protocol, while trunks 2 and 3 use the E&M Immediate Start CAS protocol.</p> <p>Note: For additional CAS table <i>ini</i> file parameters (CASFileName_0, CASFileName_1, CASFileName_7, and CASTablesNum), refer to 'E1/T1 Configuration Parameters' on page 340.</p> |
| Dial Plan [CasTrunkDialPlanName] | <p>The Dial Plan name that is used on a specific trunk.</p> <p>The range is up to 11 character strings.</p> |
| Miscellaneous | |
| PSTN Alert Timeout [TrunkPSTNAlertTimeout_ID] | <p>Alert Timeout (ISDN T301 timer) in seconds for outgoing calls to PSTN. This timer is used between the time that SETUP is sent to the Tel side (IP-to-Tel call establishment) and CONNECT is received. If ALERT is received, the timer is restarted.</p> <p>The ID is the trunk number (0 - 3).</p> <p>The range is 1 to 600. The default is 180 seconds.</p> |
| Play Ringback Tone to Trunk [PlayRBTone2Trunk_ID] | <p>ID = Trunk number (0-73).</p> <ul style="list-style-type: none"> ▪ [0] Don't Play = The ISDN / CAS gateway doesn't play a Ringback Tone (RBT). No PI is sent to the ISDN, unless the parameter 'Progress Indicator to ISDN' is configured differently. ▪ [1] Play on Local = The CAS gateway plays a local RBT to PSTN after receipt of a 180 ringing response (with or without SDP). <p>Note: Reception of a 183 response doesn't cause the CAS gateway to play an RBT (unless SIP183Behavior = 1). The ISDN gateway functions according to the parameter LocalISDNRBSrc:</p> <p>1) If the ISDN gateway receives a 180 ringing response (with or without SDP) and LocalISDNRBSrc = 1, it plays a RBT and sends an Alert with PI = 8 (unless the parameter 'Progress Indicator to ISDN' is configured differently).</p> <p>2) If LocalISDNRBSrc = 0, the ISDN gateway doesn't play an RBT and an Alert message (without PI) is sent to the ISDN. In this case, the PBX / PSTN should play the RBT to the originating terminal by itself.</p> <p>Note: Reception of a 183 response doesn't cause the ISDN gateway to play an RBT; the gateway issues a Progress message (unless SIP183Behavior = 1). If SIP183Behavior = 1, the 183 response is treated the same way as a 180 ringing response.</p> |

Table 5-43: E1/T1/J1 Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|--|
| | <ul style="list-style-type: none"> [2] Prefer IP = Play according to 'early media' (default). If a 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the ISDN / CAS gateway doesn't play the RBT; PI = 8 is sent in an ISDN Alert message (unless the parameter 'Progress Indicator to ISDN' is configured differently). If a 180 response is received but the 'early media' voice channel is not opened, the CAS gateway plays an RBT to the PSTN; the ISDN gateway functions according to the parameter LocalISDNRBSource: <ul style="list-style-type: none"> 1) If LocalISDNRBSource = 1, the ISDN gateway plays an RBT and sends an ISDN Alert with PI = 8 to the ISDN (unless the parameter 'Progress Indicator to ISDN' is configured differently). 2) If LocalISDNRBSource = 0, the ISDN gateway doesn't play an RBT. No PI is sent in the ISDN Alert message (unless the parameter 'Progress Indicator to ISDN' is configured differently). In this case, the PBX / PSTN should play an RBT tone to the originating terminal by itself. <p>Note: Reception of a 183 response results in an ISDN Progress message (unless SIP183Behavior = 1). If SIP183Behavior = 1 (183 is handled in the same way as a 180 + SDP), the gateway sends an Alert message with PI = 8, without playing an RBT.</p> |
| Transfer Mode [TrunkTransferMode] | Enables the trunk Transfer Mode. Refer to TrunkTransferMode (0, 1, or 3) in 'ISDN and CAS Interworking-Related Parameters' on page 343. Note: This parameter is only available for Protocol Type T1 CAS. |
| Enable TBCT [TrunkTransferMode] | Enables the TBCT trunk transfer mode. Refer to TrunkTransferMode (0 and 2) in 'ISDN and CAS Interworking-Related Parameters' on page 343. Note: This parameter is only available for Protocol Type T1 N12 ISDN. |
| Enable RLT [TrunkTransferMode] | Enables the RLT trunk transfer mode. Refer to TrunkTransferMode (0 and 2) in 'ISDN and CAS Interworking-Related Parameters' on page 343. Note: This parameter is only available for Protocol Type T1 DMS100 ISDN. |
| Enable Single Step Transfer [TrunkTransferMode] | Enables the Single Step Transfer trunk transfer mode. Refer to TrunkTransferMode (0 and 4) in 'ISDN and CAS Interworking-Related Parameters' on page 343. Note: This parameter is only available for Protocol Type T1 QSIG. |
| Enable ECT [TrunkTransferMode] | Enables the ECT trunk transfer mode. Refer to TrunkTransferMode (0 and 2) in 'ISDN and CAS Interworking-Related Parameters' on page 343. Note: This parameter is only available for Protocol Type E1 EURO ISDN. |

5.8.1.2 CAS State Machines

The 'CAS State Machine Table' screen allows you to modify various timers and other basic parameters to define the initialization of the CAS state machine without changing the state machine itself (no compilation is needed). The change doesn't affect the state machine itself but rather the configuration.

➤ **To modify the CAS state machine parameters, take these 6 steps:**

1. Open the 'CAS State Machine Table' screen (**Advanced Configuration** menu > **PSTN Settings** > **CAS State Machine**).

Figure 5-47: CAS State Machine Table Screen

| CAS State Machine Table | | | | | | | | | |
|------------------------------------|------------------------|---------------------------|-------------------------|-------------------------|-----------------------------|-------------------------|-------------|------------------------|----------------|
| CAS Table Name | Generate Digit On Time | Generate Inter Digit Time | DTMF Max Detection Time | DTMF Min Detection Time | Max Incoming Address Digits | Max Incoming ANI Digits | Collect ANI | Digit Signaling System | Related Trunks |
| E_M_WinkTable.dat | -1 | -1 | -1 | -1 | -1 | -1 | Default ▾ | Default ▾ | |
| E_M_WinkTable_A-Bit for E1 cas.dat | -1 | -1 | -1 | -1 | -1 | -1 | Default ▾ | Default ▾ | |
| E_M_WinkTable - for T1 cas.dat | -1 | -1 | -1 | -1 | -1 | -1 | Default ▾ | Default ▾ | 1 |

2. Ensure that the trunk is inactive. The trunk number displayed in the 'Related Trunks' field must be green. If it is red (indicating that the trunk is active), click the trunk number to open the 'Trunk Settings' screen (refer to 'Trunk Settings' on page 206), select the required Trunk number icon, and then click **Stop Trunk**.
3. In the 'CAS State Machine Table' screen, modify the required parameters according to the table below.
4. Activate the trunk if required in the 'Trunk Settings' screen by clicking the trunk number in the 'Related Trunks' field, and in the 'Trunk Settings' screen (refer to 'Trunk Settings' on page 206), select the required Trunk number icon, and then click **Apply Trunk Settings**.
5. Click **Submit**.
6. Reset the gateway and save your settings to the flash memory (refer to 'Resetting the Gateway' on page 279).


Notes:

- It's strongly recommended that you don't modify the default values unless you fully understand the implications of the changes and know the default values. Every change affects the configuration of the state machine parameters and the call process related to the trunk you are using with this state machine.
- You can only modify CAS state machine parameters if the following conditions are met:
 - 1) Trunks are inactive (stopped), i.e., trunk number displayed in green in the 'Related Trunks' field.
 - 2) State machine is not in use or in reset, or when it is not related to any trunk. In case it is related to a trunk, you must delete the trunk or deactivate (*Stop*) the trunk.
- Field values displaying '-1' indicate CAS default values. In other words, CAS state machine values are used.
- The modification of the CAS state machine occurs at the CAS application initialization only for non-default values (-1).
- For a detailed description of the CAS Protocol table, refer to the *SIP Series Reference Manual*.

Table 5-44: CAS State Machine Parameters

| Parameter | Description |
|--|---|
| Generate Digit On Time [CasStateMachineGenerateDigitOnTime] | Generates digit on-time (in msec). The value must be a positive value. The default value is -1. |
| Generate Inter Digit Time [CasStateMachineGenerateInterDigitTime] | Generates digit off-time (in msec). The value must be a positive value. The default value is -1. |
| DTMF Max Detection Time [CasStateMachineDTMFMaxOnDetectionTime] | Detects digit maximum on time (according to DSP detection information event) in msec units. The value must be a positive value. The default value is -1. |
| DTMF Min Detection Time [CasStateMachineDTMFMinOnDetectionTime] | Detects digit minimum on time (according to DSP detection information event) in msec units. The digit time length must be longer than this value to receive a detection. Any number may be used, but the value must be less than CasStateMachineDTMFMaxOnDetectionTime. The value must be a positive value. The default value is -1. |
| MAX Incoming Address Digits [CasStateMachineMaxNumOfIncomingAddressDigits] | Defines the limitation for the maximum address digits that need to be collected. After reaching this number of digits, the collection of address digits is stopped. The value must be an integer. The default value is -1. |
| MAX Incoming ANI Digits [CasStateMachineMaxNumOfIncomingANIDigits] | Defines the limitation for the maximum ANI digits that need to be collected. After reaching this number of digits, the collection of ANI digits is stopped. The value must be an integer. The default value is -1. |

Table 5-44: CAS State Machine Parameters

| Parameter | Description |
|---|--|
| Collet ANI [CasStateMachineCollectANI] | In some cases, when the state machine handles the ANI collection (not related to MFCR2), you can control the state machine to collect ANI or discard ANI. <ul style="list-style-type: none"> ▪ [0] No = Don't collect ANI. ▪ [1] Yes = Collect ANI. ▪ [-1] Default = Default value. |
| Digit Signaling System [CasStateMachineDigitSignalingSystem] | Defines which Signaling System to use in both directions (detection\generation). <ul style="list-style-type: none"> ▪ [0] DTMF = Uses DTMF signaling. ▪ [1] MF = Uses MF signaling (default). ▪ [-1] Default = Default value. |

5.8.2 Configuring the TDM Bus Settings

➤ To configure the TDM Bus Settings parameters, take these 5 steps:

1. Open the 'TDM Bus Settings' screen (**Advanced Configuration** menu > **TDM Bus Settings**).

Figure 5-48: TDM Bus Settings Screen

| TDM Bus Settings | |
|-----------------------------------|---------|
| ! PCM Law Select | ALaw |
| TDM Bus Type | Framers |
| ! Idle PCM Pattern | 85 |
| ! Idle ABCD Pattern | 0x0F |
| TDM Bus Local Reference | 1 |
| TDM Bus PSTN Auto Clock | Disable |
| TDM Bus PSTN Auto Clock Reverting | Disable |
| TDM Bus Clock Source | Network |

2. Configure the TDM Bus Settings parameters.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.
5. A device reset is required to activate the TDM Bus Settings parameters. To reset the gateway, refer to 'Resetting the Gateway' on page 279.



Note: Usually the 'PCM Law Select' parameter is set to A-law for E1 trunks and to μ -law for T1 trunks.

Refer to 'Clock Settings' on page 439 for information on configuring the 'TDM Bus Clock Source', 'TDM Bus Enable Fallback' and 'TDM Bus PSTN Auto Clock' parameters.

Table 5-45: TDM Bus Settings Parameters

| Parameter | Description |
|---|---|
| PCM Law Select [PCMLawSelect] | <ul style="list-style-type: none"> [1] Alaw = Alaw (default) [3] MuLaw = MuLaw <p>Usually A-Law is used for E1 spans and μ-Law for T1 and J1 spans.</p> |
| TDM Bus Type [TDMBusType] | N/A. |
| Idle PCM Pattern [IdlePCMPattern] | <p>Defines the PCM Pattern that is applied to E1/T1 timeslot (B-channel) when the channel is idle.</p> <p>The range is 0 to 255. The default is set internally according to the Law select 1 (0xFF for Mu-Law; 0x55 for A-law).</p> |
| Idle ABCD Pattern [IdleABCDPattern] | <p>ABCD (CAS) Pattern to be applied to CAS signaling bus when the channel is idle.</p> <p>Range 0x0 to 0xF. Default is -1 (default pattern = 0000).</p> <p>Note: This is only relevant when using PSTN interface with CAS protocols.</p> |
| TDM Bus Local Reference [TDMBusLocalReference] | <p>0 to 3 (default = 0).</p> <p>Physical Trunk ID from which the gateway recovers its clock.</p> <p>Note: Applicable only if TDMBusClockSource = 4 and TDMBusPSTNAutoClockEnable = 0.</p> |
| TDM Bus PSTN Auto Clock [TDMBusPSTNAutoClockEnable] | <p>Enables or disables the PSTN trunk auto-fallback clock feature.</p> <ul style="list-style-type: none"> [0] Disable = Recovers the clock from the E1/T1 line defined by the parameter TDMBusLocalReference (default). [1] Enable = Recovers the clock from any connected synchronized slave E1/T1 line. If this trunk loses its synchronization, the gateway attempts to recover the clock from the next trunk. Note that initially the gateway attempts to recover the clock from the trunk defined by the parameter TDMBusLocalReference. <p>Note: This parameter is relevant only if TDMBusClockSource = 4.</p> |
| TDM Bus PSTN Auto Clock Reverting [TDMBusPSTNAutoClockRevertingEnable] | <p>Enables or disables the PSTN trunk auto-fallback reverting feature. If a trunk with a higher priority than the current LocalReference is being synchronized, the gateway LocalReference changes to the new trunk.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <p>Note: The parameter is valid only when the TDMBusPSTNAutoClockEnable parameter is set to 1.</p> |
| TDM Bus Clock Source [TDMBusClockSource] | <ul style="list-style-type: none"> [1] Internal = Generate clock from local source (default). [4] Network = Recover clock from PSTN line. <p>For detailed information on configuring the gateway's clock settings, refer to 'Clock Settings' on page 439.</p> |

5.9 Security Settings

From the **Security Settings** submenu, you can configure the following:

- Web User Accounts (refer to 'Configuring the Web User Accounts' on page [223](#))
- Web & Telnet Access List (refer to 'Configuring the Web and Telnet Access List' on page [225](#))
- Firewall Settings (refer to 'Configuring the Firewall Settings' on page [226](#))
- Certificates (refer to 'Configuring the Certificates' on page [228](#))
- General Security Settings (refer to 'Configuring the General Security Settings' on page [232](#))
- IPSec Table (refer to 'Configuring the IPSec Table' on page [236](#))
- IKE Table (refer to 'Configuring the IKE Table' on page [240](#))

5.9.1 Configuring the Web User Accounts

To prevent unauthorized access to the Embedded Web Server, two user accounts are available, a primary and secondary. Each account is composed of three attributes: username, password, and access level. For detailed information on the user account mechanism, refer to 'User Accounts' on page [58](#).

It is recommended that you change the default username and password of the account used to access the Embedded Web Server.

➤ **To change the Web User Accounts attributes, take these 4 steps:**

1. Open the 'Web User Accounts' screen (**Advanced Configuration** menu > **Security Settings** > **Web User Accounts** option).

Figure 5-49: Web User Accounts Screen (for Users with 'Security Administrator' Privileges)

| Web User Accounts | | |
|---|------------------------|---------------------|
| Current Logged User: Admin | | |
| Account Data for User: Admin | | |
| User Name | Admin | Change User Name |
| Access Level | Security Administrator | |
| Fill in the following 3 fields to change the password | | |
| Current Password | | |
| New Password | | |
| Confirm New Password | | Change Password |
| Account Data for User: - | | |
| User Name | - | Change User Name |
| Access Level | User Monitor | Change Access Level |
| Fill in the following 3 fields to change the password | | |
| Current Password | | |
| New Password | | |
| Confirm New Password | | Change Password |

2. To change the access level of the secondary account (the access level of the primary account cannot be changed), from the 'Access Level' drop-down list, select the new access level, and then click **Change Access Level**; the new access level is applied immediately.
3. To change the username of an account, enter the new username in the field 'User Name', and then click **Change User Name**; the new username is applied immediately and the 'Enter Network Password' screen appears. Enter the updated username in the 'Enter Network Password' screen. Note that the username can be a maximum of 19 case-sensitive characters.
4. To change the password of an account, enter the current password in the field 'Current Password', the new password in the fields 'New Password' and 'Confirm New Password', and then click **Change Password**; the new password is applied immediately and the 'Enter Network Password' screen appears. Enter the updated password in the 'Enter Network Password' screen. Note that the password can be a maximum of 19 case-sensitive characters.



Note: A user with a 'Security Administrator' access level can change all attributes for all accounts. Users with an access level other than 'Security Administrator' can only change their own password and username.

5.9.2 Configuring the Web and Telnet Access List

The 'Web & Telnet Access List' screen is used to define up to ten IP addresses that are permitted to access the gateway's Embedded Web Server and Telnet interfaces. Access from an undefined IP address is denied. If no IP addresses are defined, this security feature is inactive and the gateway can be accessed from any IP address.

The Web and Telnet Access List can also be defined using the *ini* file parameter WebAccessList_x (refer to 'Web and Telnet Parameters' on page 315).

➤ **To add authorized IP addresses for Embedded Web Server and Telnet access, take these 4 steps:**

1. Open the 'Web & Telnet Access List' screen (**Advanced Configuration** menu > **Security Settings** > **Web & Telnet Access List** option).

Figure 5-50: Web & Telnet Access List Screen

| Delete Row | Authorized IP Address |
|------------|-----------------------|
| 1 | 10.13.2.66 |
| 2 | 10.33.45.68 |

Delete Selected Addresses

Note: Delete all rows to allow access from any IP address.

Add a new IP address authorized to connect to the device's web and telnet interfaces.

New Authorized IP Address

Add New Address

2. To add an authorized IP address, in the 'New Authorized IP Address' field, enter the required IP address (refer to Note 1 below), and then click **Add New Address**; the IP address you entered is added as a new entry to the Web & Telnet Access List table.
3. To delete authorized IP addresses, select the Delete Row check box corresponding to the IP addresses that you want to delete (refer to Note 2 below), and then click **Delete Selected Addresses**; the IP addresses are removed from the table and can no longer access the Web and Telnet interfaces.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.



Notes:

- The first authorized IP address in the list must be your terminal's IP address; otherwise, access from your terminal is denied.
- Delete your terminal's IP address last from the 'Web & Telnet Access List' screen. If it's deleted before the last, access from your terminal is denied after it's deleted.

5.9.3 Configuring the Firewall Settings

The gateway accommodates an internal Firewall, allowing the security administrator to define network traffic filtering rules. For detailed information on the internal Firewall, refer to the *SIP Series Reference Manual*.

➤ **To create a new access firewall rule, take these 6 steps:**

1. Open the 'Firewall Settings' screen (**Advanced Configuration** menu > **Security Settings** > **Firewall Settings** option).

Figure 5-51: Firewall Settings Screen

| Firewall Settings | | | | | | | | | | | |
|-------------------|----------------------------------|-----------|-------------------|------------------|-------------|-------------|-----------|-------------|-------------------|-------------|---|
| Selected Rule | Is Rule Active? | Source IP | Mask | Local Port Range | Protocol | Packet Size | Byte rate | Burst Bytes | Action Upon Match | Match Count | |
| 0 | <input type="radio"/> | No | mgmt.customer.com | 255.255.255.255 | 0-80 | tcp | 0 | 0 | 0 | ALLOW | 0 |
| 1 | <input type="radio"/> | No | 192.0.0.0 | 255.0.0.0 | 0-65535 | Any | 0 | 40000 | 50000 | BLOCK | 0 |
| 2 | <input checked="" type="radio"/> | Yes | 10.31.4.0 | 255.255.255.0 | 4000 - 9000 | Any | 0 | 0 | 0 | Block | 0 |
| 3 | <input type="radio"/> | Yes | 10.4.0.0 | 255.255.0.0 | 4000-9000 | Any | 0 | 0 | 0 | BLOCK | 0 |

2. In the 'New Rule Index' field, enter the index of the access rule that you want to add.
3. Click the **Add an Empty Rule** button; a new rule appears; alternatively, click the **Copy Selected Rule as a New Rule** button; a new rule that is an exact copy of the currently selected rule appears.
4. Configure the rule's parameters according to the table below.
5. Click one of the following buttons:
 - **Apply Rule Settings** to save the new rule (the rule isn't active).
 - **Activate Rule** to save the new rule and activate it.
 - **Delete Rule** to delete the rule.
6. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

➤ **To edit a rule, take these 5 steps:**

1. Select the radio button of the entry you want to edit.
2. Click the **Make Rule Editable** button; the rule's fields can now be modified.
3. Modify the fields according to your requirements.
4. Click the **Apply Rule Settings** button to save the changes.
5. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

➤ **To activate a de-activated rule, take these 2 steps:**

1. Select the radio button of the entry you want to activate.
2. Click the **Activate Rule** button; the rule is active.

➤ **To de-activate an activated rule, take these 2 steps:**

1. Select the radio button of the entry you want to activate.
2. Click the **DeActivate Rule** button; the rule is de-activated.

➤ **To delete a rule, take these 3 steps:**

1. Select the radio button of the entry you want to activate.
2. Click the **Delete Rule** button; the rule is deleted.
3. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-46: Internal Firewall Parameters

| Parameter | Description |
|--|--|
| Is Rule Active | A read-only field that indicates whether the rule is active or not. Note: After reset all rules are active. |
| Source IP [AccessList_Source_IP] | IP address (or DNS name) of source network, or a specific host. |
| Mask [AccessList_Net_Mask] | IP network mask. 255.255.255.255 for a single host or the appropriate value for the source IP addresses. The IP address of the sender of the incoming packet is bitwise ANDed with this mask and then compared to the field 'Source IP'. |
| Local Port Range [AccessList_Start_Port] [AccessList_End_Port] | The destination UDP/TCP ports (on this device) to which packets are sent. The valid range is 0 to 65535. Note: When the protocol type isn't TCP or UDP, the entire range must be provided. |
| Protocol [AccessList_Protocol] | The protocol type (e.g., UDP, TCP, ICMP, ESP or 'Any'), or the IANA protocol number (in the range of 0 (Any) to 255). Note: The protocol field also accepts the abbreviated strings 'SIP' and 'HTTP'. Specifying these strings implies selection of the TCP or UDP protocols, and the appropriate port numbers as defined on the device. |
| Packet Size [AccessList_Packet_Size] | Maximum allowed packet size. The valid range is 0 to 65535. Note: When filtering fragmented IP packets, the 'Packet Size' field relates to the overall (reassembled) packet size, not to the size of each fragment. |
| Byte Rate [AccessList_Byte_Rate] | Expected traffic rate (bytes per second). |
| Burst Bytes [AccessList_Byte_Burst] | Tolerance of traffic rate limit (number of bytes). |
| Action Upon Match [AccessList_Allow_Type] | Action upon match (Allow or Block). |
| Match Count [AccessList_MatchCount] | A read-only field that provides the number of packets accepted / rejected by a specific rule. |

5.9.4 Configuring the Certificates

The 'Certificates' screen is used to replace the server (refer to 'Server Certificate Replacement' on page 228) and client (refer to 'Client Certificates' on page 229) certificates and to update the private key (using HTTPSPkeyFileName, as described in the *SIP Series Reference Manual*).

5.9.4.1 Server Certificate Replacement

The gateway is supplied with a working SSL configuration consisting of a unique self-signed server certificate. If an organizational Public Key Infrastructure (PKI) is used, you may wish to replace this certificate with one provided by your security administrator.

➤ **To replace the gateway self-signed certificate, take these 8 steps:**

1. Your network administrator should allocate a unique DNS name for the gateway (e.g., dns_name.corp.customer.com). This name is used to access the device, and should therefore be listed in the server certificate.
2. Open the 'Certificates Signing Request' screen (**Advanced Configuration** menu > **Security Settings** submenu > **Certificates** option).

Figure 5-52: Certificates Signing Request Screen



Certificate Signing Request

Subject Name

Generate CSR

Copy the certificate signing request and send it to your Certification Authority for signing.

Press the button "Generate self-signed" to create a self-signed certificate using the subject name provided above.
Important: this is a lengthy operation, during this time the device will be out of service.
 After the operation is complete, save configuration and reset the device.

Generate self-signed

Certificate Files

Send "Server Certificate" file from your computer to the device

Send File **Browse...**

Send "Trusted Root Certificate Store" file from your computer to the device

Send file **Browse...**

Send "Private Key" file from your computer to the device

Send file **Browse...**

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

3. In the 'Subject Name' field, enter the DNS name, and then click **Generate CSR**. A textual certificate signing request, that contains the SSL device identifier, is displayed.
4. Copy this text and send it to your security provider; the security provider (also known as Certification Authority or CA) signs this request and send you a server certificate for the device.
5. Save the certificate in a file (e.g., cert.txt). Ensure the file is a plain-text file with the 'BEGIN CERTIFICATE' header. Below is an example of a Base64-Encoded X.509 Certificate.

```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJGUj
ETMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBTZXJ2ZXVY
MB4XDTk4MDYyNDA4MDAwMFOXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRlIxEz
ARBgNVBAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9zdGUgU2VydMv1cjCC
ASEwDQYJKoZIhvcNAQEBBQADggEAOADCCAQkCggEAPqd4MziR4spWldGRx8bQrhZkon
WnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfX7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7
JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRefiXDmuOe+FhJ
gHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END CERTIFICATE-----
```

6. Before continuing, set the parameter HTTPOnly to 0 to ensure you have a method of accessing the device in case the new certificate doesn't work. Restore the previous setting after testing the configuration.
7. In the 'Certificates Files' pane, click the **Browse** button corresponding to 'Send Server Certificate...', navigate to the cert.txt file, and then click **Send File**.
8. When the operation is completed, save the configuration (refer to 'Saving Configuration' on page 278) and restart the gateway; the Embedded Web Server uses the provided certificate.



Notes:

- The certificate replacement process can be repeated when necessary (e.g., the new certificate expires).
- It is possible to use the IP address of the gateway (e.g., 10.3.3.1) instead of a qualified DNS name in the Subject Name. This is not recommended since the IP address is subject to changes and may not uniquely identify the device.
- The server certificate can also be loaded via *ini* file using the parameter HTTPSCertFileName.

5.9.4.2 Client Certificates

By default, Web servers using SSL provide one-way authentication. The client is certain that the information provided by the Web server is authentic. When an organizational PKI is used, two-way authentication may be desired: both client and server should be authenticated using X.509 certificates. This is achieved by installing a client certificate on the managing PC, and loading the same certificate (in base64-encoded X.509 format) to the gateway Trusted Root Certificate Store. The Trusted Root Certificate file should contain both the certificate of the authorized user and the certificate of the CA.

Since X.509 certificates have an expiration date and time, the gateway must be configured to use NTP (refer to 'Simple Network Time Protocol Support' on page 430) to obtain the current date and time. Without a correct date and time, client certificates cannot work.

➤ **To enable two-way client certificates, take these 6 steps:**

1. Before continuing, set HTTPSEnabled to 0 to ensure you have a method of accessing the device in case the client certificate doesn't work. Restore the previous setting after testing the configuration.
2. Open the 'Certificates Signing Request' screen (**Advanced Configuration** menu > **Security Settings** submenu > **Certificates** option); the 'Certificates Signing Request' screen is displayed (refer to 'Server Certificate Replacement' on page 228).
3. To load the Trusted Root Certificate file, locate the trusted root certificate loading section.
4. Click **Browse**, navigate to the file, and then click **Send File**.
5. When the operation is completed, set the *ini* file parameter, HTTPSRequireClientCertificates to 1.
6. Save the configuration (refer to 'Saving Configuration' on page 278), and then restart the gateway.

When a user connects to the secure Web server:

- If the user has a client certificate from a CA listed in the Trusted Root Certificate file, the connection is accepted and the user is prompted for the system password.
- If both the CA certificate and the client certificate appear in the Trusted Root Certificate file, the user is not prompted for a password (thus providing a single-sign-on experience - the authentication is performed using the X.509 digital signature).
- If the user doesn't have a client certificate from a listed CA, or doesn't have a client certificate at all, the connection is rejected.



Notes:

- The process of installing a client certificate on your PC is beyond the scope of this document. For more information, refer to your Web browser or operating system documentation, and/or consult your security administrator.
- The root certificate can also be loaded via *ini* file using the parameter HTTPSRootFileName.

5.9.4.3 Self-Signed Certificates

The gateway is shipped with a operational, self-signed server certificate. The subject name for this default certificate is 'ACL_nnnnnnn', where *nnnnnnn* denotes the serial number of the gateway. However, this subject name may not be appropriate for production and can be changed while still using self-signed certificates.

➤ **To change the subject name and regenerate the self-signed certificate, take these steps:**

1. Before you begin, ensure the following:
 - You have a unique DNS name for the gateway (e.g., `dns_name.corp.customer.com`). This name is used to access the gateway and should therefore, be listed in the server certificate.
 - No traffic is running on the gateway. The certificate generation process is disruptive to traffic and should be executed during maintenance time.
2. Open the 'Certificates' screen (**Advanced Configuration** menu > **Security Settings** submenu > **Certificates** option); the 'Certificates Signing Request' screen is displayed (refer to 'Server Certificate Replacement' on page 228).
3. In the 'Subject Name' field, enter the fully-qualified DNS name (FQDN) as the certificate subject, and then click **Generate Self-signed**; after a few seconds, a message appears displaying the new subject name.
4. Save configuration (refer to 'Saving Configuration' on page 278), and then restart the device for the new certificate to take effect.

Alternatively, the self-signed server certificate may be regenerated (e.g., using the subject name "dns_name.corp.customer.com"), using the CLI command **CertificateMgmt** (CM) in the CONFiguration directory:

```
/> /CONF/CM GENERATE dns_name.corp.customer.com
```

➤ **To export the current server certificate to a file using Microsoft Internet Explorer, take these 6 steps:**

1. Access the gateway's Embedded Web Server.
2. Double-click the yellow padlock icon displayed at the bottom of the Browser's window.
3. Select the 'Details' tab, and then click **Copy to file**.
4. Click **Next**, select 'Base64-encoded X.509', and then click **Next**.
5. Select a file name, and then click **Next**.
6. Click **Finish**; the certificate is saved to the selected file name.

To export the current server certificate using CLI, type: `/> /CONF/CM GETCERT`

The server certificate is displayed in base64-encoded PEM format.

5.9.5 Configuring the General Security Settings

The 'General Security Settings' screen is used to configure various security features.

➤ **To configure the general security parameters, take these 4 steps:**

1. Open the 'General Security Settings' screen (**Advanced Configuration** menu > **Security Settings** > **General Security Settings** option).

Figure 5-53: General Security Settings Screen

| General Security Settings | |
|---|---------------------------|
| Secured Web Connection (HTTPS) | HTTP and HTTPS ▾ |
| HTTP Authentication Mode | Digest when possible ▾ |
| ! TLS version | SSL 2.0-3.0 and TLS 1.0 ▾ |
| Voice Menu Password | ••••• |
| General RADIUS Settings | |
| ! Enable RADIUS Access Control | Disable ▾ |
| Use RADIUS for Web/Telnet Login | Disable ▾ |
| ! RADIUS Authentication Server IP Address | 0.0.0.0 |
| ! RADIUS Authentication Server Port | 1645 |
| ! RADIUS Shared Secret | •••••••••• |
| RADIUS Authentication Settings | |
| Default Access Level | 200 |
| Device Behavior Upon RADIUS Timeout | Verify Access Locally ▾ |
| Local RADIUS Password Cache Mode | Reset Timer Upon Access ▾ |
| Local RADIUS Password Cache Timeout [sec] | 300 |
| RADIUS VSA Vendor ID | 5003 |
| RADIUS VSA Access Level Attribute | 35 |
| EtherDiscover Settings | |
| EtherDiscover Operation Mode | Enable if unconfigured ▾ |
| SRTP Settings | |
| Enable Media Security | Disable ▾ |
| Media Security Behavior | Mandatory ▾ |
| IPSec Settings | |
| Enable IP Security | Disable ▾ |

2. Configure the General Security Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-47: General Security Settings Parameters

| Parameter | Description |
|---|---|
| Secured Web Connection [HTTPSOnly] | <p>Determines the protocol types used to access the Embedded Web Server.</p> <ul style="list-style-type: none"> [0] HTTP and HTTPS (default). [1] HTTPS only = Unencrypted HTTP packets are blocked. |
| HTTP Authentication Mode [WebAuthMode] | <p>Determines the authentication mode for the Embedded Web Server.</p> <ul style="list-style-type: none"> [0] Basic = Basic authentication (clear text) is used (default). [1] Digest When Possible = Digest authentication (MD5) is used. [2] Basic if HTTPS, Digest if HTTP = Digest authentication (MD5) is used for HTTP, and basic authentication is used for HTTPS. <p>Note: When RADIUS login is enabled (WebRADIUSLogin = 1), basic authentication is forced.</p> |
| TLS version [TLSVersion] | <p>Defines the supported versions of SSL/TLS (Secure Socket Layer/Transport Layer Security).</p> <ul style="list-style-type: none"> [0] SSL 2.0-3.0 and TLS 1.0 = SSL 2.0, SSL 3.0, and TLS 1.0 are supported (default). [1] TLS 1.0 Only = only TLS 1.0 is used. <p>When set to [0], SSL/TLS handshakes always start with SSL 2.0 and switch to TLS 1.0 if both peers support it. When set to [1], TLS 1.0 is the only version supported; clients attempting to contact the device using SSL 2.0 are rejected.</p> |
| Voice Menu Password [VoiceMenuPassword] | <p>Password for the voice menu used for configuration and status. To activate the menu, connect an analog telephone and dial *** (three stars) followed by the password.</p> <p>The default value is 12345.</p> <p>For detailed information on the voice menu, refer to Assigning an IP Address Using the Voice Menu Guidance on page 52.</p> |
| RADIUS General Settings | |
| Enable RADIUS Access Control [EnableRADIUS] | <p>Enables / disables the RADIUS application.</p> <ul style="list-style-type: none"> [0] Disable = RADIUS application is disabled (default). [1] Enable = RADIUS application is enabled. |

Table 5-47: General Security Settings Parameters

| Parameter | Description |
|---|--|
| Use RADIUS for Web/Telnet Login [WebRADIUSLogin] | <p>Uses RADIUS queries for Web and Telnet interface authentication.</p> <ul style="list-style-type: none"> [0] Disable (default). [1] Enable. <p>When enabled, logging in to the gateway's Web and Telnet embedded servers is performed via a RADIUS server. The gateway contacts a predefined server and verifies the given username and password pair against a remote database, in a secure manner.</p> <p>Notes:</p> <ul style="list-style-type: none"> The parameter EnableRADIUS must be set to 1. RADIUS authentication requires HTTP basic authentication, meaning the username and password are transmitted in clear text over the network. Therefore, it's recommended to set the parameter HttpsOnly to 1 to force the use of HTTPS, since the transport is encrypted. |
| RADIUS Authentication Server IP Address [RADIUSAuthServerIP] | IP address of the RADIUS authentication server. |
| RADIUS Authentication Server Port [RADIUSAuthPort] | Port number of the RADIUS authentication server. The default value is 1645. |
| RADIUS Shared Secret [SharedSecret] | 'Secret' used to authenticate the gateway to the RADIUS server. Should be a cryptographically strong password. |
| RADIUS Authentication Settings | |
| Default Access Level [DefaultAccessLevel] | Defines the default access level for the gateway when the RADIUS (authentication) response doesn't include an access level attribute. The valid range is 0 to 255. The default value is 200 (Security Administrator'). |
| Local RADIUS Password Cache Mode [RadiusLocalCacheMode] | <p>Defines the gateway's mode of operation regarding the timer (configured by the parameter RadiusLocalCacheTimeout) that determines the validity of the username and password (verified by the RADIUS server).</p> <ul style="list-style-type: none"> [0] Absolute Expiry Timer = when you access a Web screen, the timeout doesn't reset but rather continues decreasing. [1] Reset Timer Upon Access = upon each access to a Web screen, the timeout always resets (reverts to the initial value configured by RadiusLocalCacheTimeout). |
| Local RADIUS Password Cache Timeout [RadiusLocalCacheTimeout] | <p>Defines the time (in seconds) the locally stored username and password (verified by the RADIUS server) are valid. When this time expires, the username and password becomes invalid and a must re-verified with the RADIUS server. The valid range is 1 to 0xFFFFFFFF. The default value is 300 (5 minutes).</p> <ul style="list-style-type: none"> [-1] = Never expires. [0] = Each request requires RADIUS authentication. |

Table 5-47: General Security Settings Parameters

| Parameter | Description |
|--|---|
| RADIUS VSA Vendor ID [RadiusVSAVendorID] | Defines the vendor ID the gateway accepts when parsing a RADIUS response packet. The valid range is 0 to 0xFFFFFFFF. The default value is 5003. |
| RADIUS VSA Access Level Attribute [RadiusVSAAccessAttribute] | Defines the code that indicates the access level attribute in the Vendor Specific Attributes (VSA) section of the received RADIUS packet. The valid range is 0 to 255. The default value is 35. |
| EtherDiscover Settings | |
| EtherDiscover Operation Mode | N/A. |
| SRTP Settings | |
| Enable Media Security [EnableMediaSecurity] | Enables or disables the Secure Real-Time Transport Protocol (SRTP). <ul style="list-style-type: none"> [0] Disable = SRTP is disabled (default). [1] Enable = SRTP is enabled. |
| Media Security Behavior [MediaSecurityBehaviour] | Determines the gateway's mode of operation when SRTP is used (EnableMediaSecurity = 1). <ul style="list-style-type: none"> [0] Preferable = The gateway initiates encrypted calls. If negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted. [1] Mandatory = The gateway initiates encrypted calls. If negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected (default). |
| IPSec Settings | |
| Enable IP Security [EnableIPSec] | Enables / disables the Secure Internet Protocol (IPSec) on the gateway. <ul style="list-style-type: none"> [0] Disable = IPSec is disabled (default). [1] Enable = IPSec is enabled. |

5.9.6 Configuring the IPSec Table

The 'IPSec Table' screen is used to configure the IPSec SPD (Security Policy Database) parameters.

➤ **To configure the IPSec SPD table using the Embedded Web Server, take these 6 steps:**

1. Access the Embedded Web Server (refer to 'Accessing the Embedded Web Server' on page 60).
2. Open the 'IPSec Table' screen (**Advanced Configuration** menu > **Security Settings** > **IPSec Table** option).

Figure 5-54: IPSec Table Screen

| IPSec Table | |
|-------------------------------------|------------------------------------|
| Policy Index | 0 State: Does not exist ▼ |
| IPSec table row does not exist | |
| Remote IP Address | <input type="text"/> |
| Local IP Address Type | Control ▼ |
| Source Port | <input type="text" value="0"/> |
| Destination Port | <input type="text" value="0"/> |
| Protocol | <input type="text" value="0"/> |
| Related Key Exchange Method Index | <input type="text" value="0"/> |
| SA Lifetime [sec] | <input type="text" value="28800"/> |
| SA Lifetime [KB] | <input type="text" value="0"/> |
| First Proposal Encryption Type | Not Defined ▼ |
| First Proposal Authentication Type | Not Defined ▼ |
| Second Proposal Encryption Type | Not Defined ▼ |
| Second Proposal Authentication Type | Not Defined ▼ |
| Third Proposal Encryption Type | Not Defined ▼ |
| Third Proposal Authentication Type | Not Defined ▼ |
| Fourth Proposal Encryption Type | Not Defined ▼ |
| Fourth Proposal Authentication Type | Not Defined ▼ |

3. From the 'Policy Index' drop-down list, select the rule you want to edit (up to 20 rules can be configured).
4. Configure the IPSec SPD parameters according to the table below.
5. Click the button **Create**; a row is added in the IPSec table.
6. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-48: IPSec SPD Table Configuration Parameters

| Parameter Name | Description |
|---|---|
| Remote IP Address [IPSecPolicyRemoteIPAddress] | Defines the destination IP address (or a FQDN) the IPSec mechanism is applied to. This parameter is mandatory. Note: When an FQDN is used, a DNS server must be configured (DNSPriServerIP). |
| Local IP Address Type [IPSecPolicyLocalIPAddressType] | Determines the local interface to which the encryption is applied (applicable to multiple IPs and VLANs). <ul style="list-style-type: none"> [0] OAM = OAM interface (default). [1] Control = Control interface. |
| Source Port [IPSecPolicySrcPort] | Defines the source port the IPSec mechanism is applied to. The default value is 0 (any port). |
| Destination Port [IPSecPolicyDstPort] | Defines the destination port the IPSec mechanism is applied to. The default value is 0 (any port). |
| Protocol [IPSecPolicyProtocol] | Defines the protocol type the IPSec mechanism is applied to. <ul style="list-style-type: none"> 0 = Any protocol (default). 17 = UDP. 6 = TCP. Any other protocol type defined by IANA (Internet Assigned Numbers Authority). |
| Related Key Exchange Method Index [IPsecPolicyKeyExchangeMethodIndex] | Determines the index for the corresponding IKE entry. Note that several policies can be associated with a single IKE entry. The valid range is 0 to 19. The default value is 0. |
| IKE Second Phase Parameters (Quick Mode) | |
| SA Lifetime (sec) [PsecPolicyLifeInSec] | Determines the time (in seconds) the SA negotiated in the second IKE session (quick mode) is valid. After the time expires, the SA is re-negotiated. The default value is 28800 (8 hours). |
| SA Lifetime (KB) [IPSecPolicyLifeInKB] | Determines the lifetime (in kilobytes) the SA negotiated in the second IKE session (quick mode) is valid. After this size is reached, the SA is re-negotiated. The default value is 0 (this parameter is ignored). |
| The lifetime parameters (IPsecPolicyLifeInSec and IPSecPolicyLifeInKB) determine the duration of which an SA is valid. When the lifetime of the SA expires, it is automatically renewed by performing the IKE second phase negotiations. To refrain from a situation where the SA expires, a new SA is being negotiated while the old one is still valid. As soon as the new SA is created, it replaces the old one. This procedure occurs whenever an SA is about to expire. | |

Table 5-48: IPSec SPD Table Configuration Parameters

| Parameter Name | Description |
|--|---|
| First to Fourth Proposal Encryption Type [IPSecPolicyProposalEncryption_X] | Determines the encryption type used in the quick mode negotiation for up to four proposals. X stands for the proposal number (0 to 3). The valid encryption values are: <ul style="list-style-type: none"> Not Defined (default) [0] None = No encryption [1] DES-CBC [2] Triple DES-CBC [3] AES-CBC |
| First to Fourth Proposal Authentication Type [IPSecPolicyProposalAuthentication_X] | Determines the authentication protocol used in the quick mode negotiation for up to four proposals. X stands for the proposal number (0 to 3). The valid authentication values are: <ul style="list-style-type: none"> Not Defined (default) [2] HMAC-SHA-1-96 [4] HMAC-MD5-96 |

If no IPSec methods are defined (Encryption / Authentication), the default settings (shown in the following table) are applied.

Table 5-49: Default IKE Second Phase Proposals

| Proposal | Encryption | Authentication |
|-------------------|------------|----------------|
| Proposal 0 | 3DES | SHA1 |
| Proposal 1 | 3DES | MD5 |
| Proposal 2 | DES | SHA1 |
| Proposal 3 | DES | MD5 |

➤ **To configure the IPSec SPD table using the *ini* file:**

- The IPSec SPD table is configured using *ini* file tables (described in 'Structure of ini File Parameter Tables' on page 295). Each line in the table refers to a different IP destination. The Format line (SPD_INDEX in the example below) specifies the order in which the actual data lines are written. The order of the parameters is irrelevant. Parameters are not mandatory unless stated otherwise. To support more than one Encryption / Authentication proposals, for *each* proposal specify the relevant parameters in the Format line. Note that the proposal list must be contiguous.

An example of an IPsec SPD Table is shown below:

```
[ IPSEC SPD TABLE ]
Format SPD INDEX = IPsecPolicyRemoteIPAddress, IpsecPolicySrcPort,
IPsecPolicyDStPort, IPsecPolicyProtocol, IPsecPolicyLifeInSec,
IPsecPolicyProposalEncryption 0,
IPsecPolicyProposalAuthentication 0,
IPsecPolicyProposalEncryption_1,
IPsecPolicyProposalAuthentication 1,
IPsecPolicyKeyExchangeMethodIndex, IPsecPolicyLocalIPAdressType;
IPSEC_SPD_TABLE 0 = 10.11.2.21, 0, 0, 17, 900, 1,2, 2,2 ,1, 0;
[ \IPSEC SPD TABLE ]
```

In the IPsec SPD example, all packets designated to IP address 10.11.2.21 that originates from the OAM interface (regardless to their destination and source ports) and whose protocol is UDP are encrypted, the IPsec SPD also defines an SA lifetime of 900 seconds and two security proposals: DES/SHA1 and 3DES/SHA1.

5.9.7 Configuring the IKE Table

The 'IKE Table' screen is used to configure the IKE parameters.

➤ **To configure the IKE table using the Embedded Web Server, take these 6 steps:**

1. Access the Embedded Web Server (refer to 'Accessing the Embedded Web Server' on page 60).
2. Open the 'IKE Table' screen (**Advanced Configuration** menu > **Security Settings** > **IKE Table** option).

Figure 5-55: IKE Table Screen

| IKE Table | |
|--|---------------------------|
| Policy Index | 0 State: Does not exist ▼ |
| 'Internet Key Exchange' table row does not exist | |
| Shared Key | •••••• |
| IKE SA LifeTime [sec] | 28800 |
| IKE SA LifeTime [KB] | 0 |
| First Proposal Encryption Type | Not Defined ▼ |
| First Proposal Authentication Type | Not Defined ▼ |
| First Proposal DH Group | Not Defined ▼ |
| Second Proposal Encryption Type | Not Defined ▼ |
| Second Proposal Authentication Type | Not Defined ▼ |
| Second Proposal DH Group | Not Defined ▼ |
| Third Proposal Encryption Type | Not Defined ▼ |
| Third Proposal Authentication Type | Not Defined ▼ |
| Third Proposal DH Group | Not Defined ▼ |
| Fourth Proposal Encryption Type | Not Defined ▼ |
| Fourth Proposal Authentication Type | Not Defined ▼ |
| Fourth Proposal DH Group | Not Defined ▼ |

3. From the 'Policy Index' drop-down list, select the peer you want to edit (up to 20 peers can be configured).
4. Configure the IKE parameters according to the parameters described in the table below. Up to two IKE main mode proposals (Encryption / Authentication / DH group combinations) can be defined. The same proposals must be configured for all peers.
5. Click **Create**; a row is create in the IKE table
6. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

To delete a peer from the IKE table, select it from the 'Policy Index' drop-down list, click the button **Delete**, and then click **OK** at the prompt.

The parameters described in the following table are used to configure the first phase (main mode) of the IKE negotiation for a specific peer. A different set of parameters can be configured for each of the 20 available peers.

Table 5-50: IKE Table Configuration Parameters

| Parameter Name | Description |
|---|--|
| Authentication Method [IkePolicyAuthenticationMethod] | <p>Determines the authentication method for IKE. The valid authentication method values include:</p> <ul style="list-style-type: none"> ▪ [0] Pre-shared Key (default) ▪ [1] RSA Signature <p>Notes:</p> <ul style="list-style-type: none"> ▪ For pre-shared key based authentication, peers participating in an IKE exchange must have a prior (out-of-band) knowledge of the common key (see IKEPolicySharedKey parameter). ▪ For RSA signature based authentication, peers must be loaded with a certificate signed by a common CA. For additional information on certificates, refer to 'Server Certificate Replacement' on page 228. |
| Shared Key [IKEPolicySharedKey] | <p>Determines the pre-shared key (in textual format). Both peers must register the same pre-shared key for the authentication process to succeed.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The pre-shared key forms the basis of IPSec security and should therefore be handled cautiously (in the same way as sensitive passwords). It is not recommended to use the same pre-shared key for several connections. ▪ Since the <i>ini</i> file is in plain text format, loading it to the gateway over a secure network connection is recommended, preferably over a direct crossed-cable connection from a management PC. For added confidentiality, use the encoded <i>ini</i> file option (described in 'Secured ini File' on page 293). ▪ After it is configured, the value of the pre-shared key cannot be obtained via Embedded Web Server, <i>ini</i> file, or SNMP (refer the <i>SIP Series Reference Manual</i>). |
| IKE SA LifeTime (sec) [IKEPolicyLifeInSec] | <p>Determines the time (in seconds) the SA negotiated in the first IKE session (main mode) is valid. After the time expires, the SA is re-negotiated. The default value is 28800 (8 hours).</p> |
| IKE SA LifeTime (KB) [IKEPolicyLifeInKB] | <p>Determines the lifetime (in kilobytes) the SA negotiated in the first IKE session (main mode) is valid. After this size is reached, the SA is re-negotiated. The default value is 0 (this parameter is ignored).</p> |
| <p>The lifetime parameters (IKEPolicyLifeInSec and IKEPolicyLifeInKB) determine the duration the SA created in the main mode phase is valid. When the lifetime of the SA expires, it's automatically renewed by performing the IKE first phase negotiations. To refrain from a situation where the SA expires, a new SA is negotiated while the old one is still valid. As soon as the new SA is created, it replaces the old one. This procedure occurs whenever an SA is about to expire.</p> | |

Table 5-50: IKE Table Configuration Parameters

| Parameter Name | Description |
|--|--|
| First to Fourth Proposal Encryption Type [IKEPolicyProposalEncryption_X] | Determines the encryption type used in the main mode negotiation for up to four proposals. X stands for the proposal number (0 to 3). The valid encryption values are: <ul style="list-style-type: none"> Not Defined (default) [1] DES-CBC [2] Triple DES-CBC [3] AES-CBC |
| First to Fourth Proposal Authentication Type [IKEPolicyProposalAuthentication_X] | Determines the authentication protocol used in the main mode negotiation for up to four proposals. X stands for the proposal number (0 to 3). The valid authentication values are: <ul style="list-style-type: none"> Not Defined (default) [2] HMAC-SHA1-96) [4] HMAC-MD5-96 |
| First to Fourth Proposal DH Group [IKEPolicyProposalDHGroup_X] | Determines the length of the key created by the DH protocol for up to four proposals. X stands for the proposal number (0 to 3). The valid DH Group values are: <ul style="list-style-type: none"> Not Defined (default) [0] DH-786-Bit [1] DH-1024-Bit |

If no IKE methods are defined (Encryption / Authentication / DH Group), the default settings (shown in the following table) are applied.

Table 5-51: Default IKE First Phase Proposals

| Proposal | Encryption | Authentication | DH Group |
|-------------------|------------|----------------|----------|
| Proposal 0 | 3DES | SHA1 | 1024 |
| Proposal 1 | 3DES | MD5 | 1024 |
| Proposal 2 | 3DES | SHA1 | 786 |
| Proposal 3 | 3DES | MD5 | 786 |

➤ **To configure the IKE table using the *ini* file, take this step:**

- The IKE parameters are configured using *ini* file tables (described in 'Structure of ini File Parameter Tables' on page 295). Each line in the table refers to a different IKE peer. The Format line (IKE_DB_INDEX in the example below) specifies the order in which the actual data lines are written. The order of the parameters is irrelevant. Parameters are not mandatory unless stated otherwise. To support more than one Encryption / Authentication / DH Group proposals, for *each* proposal specify the relevant parameters in the Format line. Note that the proposal list must be contiguous.

An example of an IKE Table is shown below:

```
[IPSec_IKEDB_Table]
Format IKE DB INDEX = IKEPolicySharedKey,
IKEPolicyProposalEncryption 0, IKEPolicyProposalAuthentication 0,
IKEPolicyProposalDHGroup 0, IKEPolicyProposalEncryption 1,
IKEPolicyProposalAuthentication 1, IKEPolicyProposalDHGroup 1,
IKEPolicyLifeInSec, IKEPolicyAuthenticationMethod;
IPSEC IKEDB TABLE 0 = 123456789, 1, 2, 0, 2, 2, 1, 28800, 0;
[IPSEC IKEDB TABLE]
```

In the example above, a single IKE peer is configured and a Pre-shared key authentication is selected. Its pre-shared key is 123456789. Two security proposals are configured: DES/SHA1/768DH and 3DES/SHA1/1024DH.

5.10 Configuring the Management Settings

The 'Management Settings' screen is used to configure the gateway's management parameters.

➤ **To configure the Management Settings parameters, take these 4 steps:**

1. Open the 'Management Settings' screen (**Advanced Configuration** menu > **Management Settings**).

Figure 5-56: Management Settings Screen

| Management Settings | |
|---|---|
| Syslog Settings | |
| Syslog Server IP Address | 10.8.2.27 |
| Syslog Server Port | 514 |
| Enable Syslog | Enable <input type="button" value="v"/> |
| Analog Ports Filter | -1 |
| Trunks Filter | -1 |
| SNMP Settings | |
| SNMP Trap Destinations | --> |
| SNMP Community String | --> |
| SNMP V3 Table | --> |
| Enable SNMP | Enable <input type="button" value="v"/> |
| Trap Manager Host Name | |
| Activity Types to Report via 'Activity Log' Messages | |
| Parameters Value Change | <input type="checkbox"/> |
| Auxiliary Files Loading | <input type="checkbox"/> |
| Device Reset | <input type="checkbox"/> |
| Flash Memory Burning | <input type="checkbox"/> |
| Device Software Update | <input type="checkbox"/> |
| Access to Restricted Domains | <input type="checkbox"/> |
| Non-Authorized Access | <input type="checkbox"/> |
| Sensitive Parameters Value Change | <input type="checkbox"/> |

2. Configure the Management Settings according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.

Table 5-52: Management Settings Parameters

| Parameter | Description |
|---|---|
| Syslog Settings | |
| Syslog Server IP address [SyslogServerIP] | <p>IP address (in dotted format notation) of the computer you are using to run the Syslog server.</p> <p>The Syslog server is an application designed to collect the logs and error messages generated by the VoIP gateway.</p> <p>Default IP address is 0.0.0.0.</p> <p>Note: Use the SyslogServerPort parameter to define the Syslog server's port.</p> <p>For information on Syslog, refer to the <i>SIP Series Reference Manual</i>.</p> |
| Syslog Server Port [SyslogServerPort] | <p>Defines the UDP port of the Syslog server.</p> <p>The valid range is 0 to 65,535. The default port value is 514.</p> <p>For information on the Syslog, refer to the <i>SIP Series Reference Manual</i>.</p> |
| Enable Syslog [EnableSyslog] | <p>Sends the logs and error message generated by the gateway to the Syslog server.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Logs and errors are not sent to the Syslog server (default). ▪ [1] Enable = Enables the Syslog server. <p>Notes:</p> <ul style="list-style-type: none"> ▪ If you enable Syslog (i.e., EnableSyslog = 1), you must enter an IP address and a port number using SyslogServerIP and SyslogServerPort parameters. ▪ Syslog messages may increase the network traffic. ▪ To configure Syslog logging levels, use the parameter GwDebugLevel. ▪ Logs are also sent to the RS-232 serial port (for information on establishing a serial communications link with the gateway, refer to Establishing a Serial Communications Link with the Mediant 1000). <p>For information on the Syslog, refer to the <i>SIP Series Reference Manual</i>.</p> |
| Analog Ports Filter | <p>Filters syslog messages pertaining to analog channels / ports specified in this field. Only syslog messages pertaining to the specified ports are reported; the rest are discarded.</p> <p>To specify a range of ports use commas (,) and / or the minus sign (-). For example: 0-3,4,6 specifies channels 0 through 3, and channels 4 and 6. To specify all ports, enter '-1'.</p> <p>Note: Syslog messages that don't include channel ID (CID) are not filtered and are received regardless of the specified channel.</p> |

Table 5-52: Management Settings Parameters

| Parameter | Description |
|---|--|
| Trunks Filter | Filters syslog messages pertaining to trunks specified in this field. Only syslog messages belonging to these trunks are reported; the rest are discarded. To specify a range of trunks, use commas (,) and / or the minus sign (-). For example: 0-3,4,6 specifies trunks 0 through 3, and trunks 4 and 6. To specify all trunks, enter '-1'. Note: Syslog messages that don't include trunk ID are not filtered and are received regardless of the specified trunk. |
| SNMP Settings | |
| For detailed information on the SNMP parameters that can be configured via the <i>ini</i> file, refer to 'SNMP Parameters' on page 321. For detailed information on developing an SNMP-based program to manage your devices, refer to the <i>SIP Series Reference Manual</i> . | |
| SNMP Trap Destinations | Refer to 'Configuring the SNMP Trap Destinations Table' on page 246. |
| SNMP Community Strings | Refer to 'Configuring the SNMP Community Strings' on page 248. |
| SNMP V3 Table | Refer to 'Configuring SNMP V3 Table' on page 249. |
| Enable SNMP [DisableSNMP] | <ul style="list-style-type: none"> [0] Enable = SNMP is enabled (default). [1] Disable = SNMP is disabled and no traps are sent. |
| Trap Manager Host Name [SNMPTrapManagerHostName] | Defines an FQDN of a remote host that is used as an SNMP manager. The resolved IP address replaces the last entry in the Trap Manager table (defined by the parameter SNMPManagerTableIP_x) and the last trap manager entry of snmpTargetAddrTable in the snmpTargetMIB. For example: 'mngr.corp.mycompany.com'. The valid range is a 99-character string. |
| Activity Types to Report via 'Activity Log' Messages | |
| The Activity Log mechanism enables the gateway to send log messages (to a Syslog server) that report certain types of web actions according to a pre-defined filter. The following filters are available: | |
| Parameters Value Change [ActivityListToLog = PVC] | Changes made on-the-fly to parameters. |
| Auxiliary Files Loading [ActivityListToLog = AFL] | Loading of auxiliary files (e.g., via Certificate screen). |
| Device Reset [ActivityListToLog = DR] | Device reset via the 'Maintenance Actions' screen. |
| Flash Memory Burning [ActivityListToLog = FB] | Burning of files / parameters to flash (e.g., 'Maintenance Actions' screen). |
| Device Software Update [ActivityListToLog = SWU] | cmp loading via the Software Upgrade Wizard. |

Table 5-52: Management Settings Parameters

| Parameter | Description |
|--|---|
| Access to Restricted Domains [ActivityListToLog = ARD] | Access to Restricted Domains. The following screens are restricted: <ul style="list-style-type: none"> ini parameters (AdminPage) General Security Settings Configuration File IPSec/IKE tables Software Upgrade Key Internal Firewall Web Access List Web User Accounts |
| Non-Authorized Access [ActivityListToLog = NAA] | Attempt to access the Embedded Web Server with a false / empty username or password. |
| Sensitive Parameters Value Change [ActivityListToLog = SPC] | Changes made to sensitive parameters: (1) IP Address (2) Subnet Mask (3) Default Gateway IP Address (4) ActivityListToLog |

5.10.1 Configuring the SNMP Trap Destinations Table

The 'SNMP Trap Destinations' screen allows you to configure the attributes of up to five SNMP managers.

➤ **To configure the SNMP Trap Destination table, take these 5 steps:**

1. Access the 'Management Settings' screen (**Advanced Configuration** menu > **Management Settings**); the 'Management Settings' screen is displayed (refer to 'Configuring the Management Settings' on page 243).
2. Open the 'SNMP Trap Destination' screen by clicking the arrow sign (-->) to the right of the SNMP Trap Destinations label.

Figure 5-57: SNMP Trap Destinations Screen

| SNMP Trap Destinations | | | |
|---|------------|-----------|-------------|
| | IP Address | Trap Port | Trap Enable |
| <input type="checkbox"/> SNMP Manager 1 | 0.0.0.0 | 162 | Enable ▼ |
| <input type="checkbox"/> SNMP Manager 2 | 0.0.0.0 | 162 | Enable ▼ |
| <input type="checkbox"/> SNMP Manager 3 | 0.0.0.0 | 162 | Enable ▼ |
| <input type="checkbox"/> SNMP Manager 4 | 0.0.0.0 | 162 | Enable ▼ |
| <input type="checkbox"/> SNMP Manager 5 | 0.0.0.0 | 162 | Enable ▼ |

3. Configure the SNMP Trap parameters according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.



Note: If you clear a check box and then click **Submit**, all settings in the same row revert to their defaults.

Table 5-53: SNMP Trap Destinations Table Parameters

| Parameter | Description |
|---|--|
| SNMP Manager [SNMPManagerIsUsed_x] | Up to five parameters, each determines the validity of the parameters (IP address and port number) of the corresponding SNMP Manager used to receive SNMP traps. <ul style="list-style-type: none"> ▪ [0] (Check box cleared) = Disabled (default) ▪ [1] (Check box selected) = Enabled |
| IP Address [SNMPManagerTableIP_x] | Up to five IP addresses of remote hosts that are used as SNMP Managers. The device sends SNMP traps to these IP addresses. Enter the IP address in dotted format notation, for example 108.10.1.255. |
| Trap Port [SNMPManagerTrapPort_x] | Up to five parameters used to define the Port numbers of the remote SNMP Managers. The device sends SNMP traps to these ports. Note: The first entry (out of the five) replaces the obsolete parameter SNMPTrapPort. The valid SNMP trap port range is 100 to 4000. The default SNMP trap port is 162. |
| Trap Enable [SNMPManagerTrapSendingEnable_x] | Up to five parameters, each determines the activation/deactivation of sending traps to the corresponding SNMP Manager. <ul style="list-style-type: none"> ▪ [0] Disable = Sending is disabled ▪ [1] Enable = Sending is enabled (default) |

5.10.2 Configuring the SNMP Community Strings

The 'SNMP Community String' screen is used to configure up to five read-only and up to five read / write SNMP community strings, and to configure the community string that is used for sending traps. For detailed information on SNMP community strings, refer to the *SIP Series Reference Manual*.

➤ **To configure the SNMP Community Strings, take these 5 steps:**

1. Access the 'Management Settings' screen (**Advanced Configuration** menu > **Management Settings**); the 'Management Settings' screen is displayed (refer to 'Configuring the Management Settings' on page 243).
2. Open the 'SNMP Community String' screen by clicking the arrow sign (-->) to the right of the SNMP Community String label.

Figure 5-58: SNMP Community Strings Screen

| SNMP Community String | | |
|--------------------------|------------------|--------------|
| Delete | Community String | Access Level |
| <input type="checkbox"/> | | Read Only |
| <input type="checkbox"/> | | Read Only |
| <input type="checkbox"/> | | Read Only |
| <input type="checkbox"/> | | Read Only |
| <input type="checkbox"/> | | Read Only |
| | | |
| <input type="checkbox"/> | | Read / Write |
| <input type="checkbox"/> | | Read / Write |
| <input type="checkbox"/> | | Read / Write |
| <input type="checkbox"/> | | Read / Write |
| <input type="checkbox"/> | | Read / Write |
| | | |
| Trap Community String | trapuser | |

3. Configure the SNMP Community Strings parameters according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to 'Saving Configuration' on page 278.



Note: To delete a community string, select the **Delete** checkbox to the left of the community string you want to delete, and then click the button **Submit**.

Table 5-54: SNMP Community Strings Parameters

| Parameter | Description |
|---|---|
| Read Only Community String [SNMPReadOnlyCommunityString_x] | Up to five read-only community strings (up to 19 characters each). The default string is 'public'. |
| Read / Write Community String [SNMPReadWriteCommunityString_x] | Up to five read / write community strings (up to 19 characters each). The default string is 'private'. |
| Trap Community String [SNMPTrapCommunityString] | Community string used in traps (up to 19 characters). The default string is 'trapuser'. |

5.10.3 Configuring SNMP V3 Users

The 'SNMP V3 Setting' screen is used to configure authentication and privacy for up to 10 SNMP v3 users.

➤ **To configure the SNMP v3 users, take the following 6 steps:**

1. Access the 'Management Settings' screen (**Advanced Configuration** menu > **Management Settings**); the 'Management Settings' screen is displayed.
2. Open the 'SNMP V3 Setting' screen by clicking the **SNMP V3 Table** arrow sign (-->).

Figure 5-59: SNMP V3 Setting Screen

| SNMP V3 Setting | | | | | | |
|-----------------|----------|--------------|--------------|---------|---------|-------|
| Index | Username | AuthProtocol | PrivProtocol | AuthKey | PrivKey | Group |
| 0 | | 0 | 0 | - | - | 1 |

3. To add an SNMP v3 user, in the 'New Row Index' field, type the desired row index, and then click **Add an Empty Row**. A new row appears.
4. Configure the SNMP V3 Setting parameters according to the table below.
5. Click the **Apply Row Settings** button to save your changes.
6. To save the changes so they are available after a hardware reset or power fail, refer to 'Saving Configuration' on page 278.



Notes:

- To delete an SNMP V3 user, select the 'Index' radio button corresponding to the SNMP V3 user that you want to delete, and then click the **Delete Row** button.
- To copy an existing SNMP V3 user configuration to a new row, select the radio button on the left of the desired SNMP V3 user, and then click **Copy Selected Row as A New Row**. A new row appears that includes the same configuration as the selected row.
- To sort all row indexes incrementally, click **Compact Table**.

Table 5-55: SNMP V3 Users Parameters

| Parameter | Description |
|--|--|
| Index [SNMPUsers_Index] | This is the table index. Its valid range is 0 to 9. |
| Username [SNMPUsers_Username] | Name of the SNMP v3 user. This name must be unique. |
| AuthProtocol [SNMPUsers_AuthProtocol] | Authentication protocol to be used for the SNMP v3 user. <ul style="list-style-type: none"> 0 = none (default) 1 = MD5 2 = SHA-1 |
| PrivProtocol [SNMPUsers_PrivProtocol] | Privacy protocol to be used for the SNMP v3 user. <ul style="list-style-type: none"> 0 = none (default) 1 = DES 2 = 3DES 3 = AES128 4 = AES192 5 = AES256 |
| AuthKey [SNMPUsers_AuthKey] | Authentication key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized. |
| PrivKey [SNMPUsers_PrivKey] | Privacy key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized. |
| Group [SNMPUsers_Group] | The group with which the SNMP v3 user is associated. <ul style="list-style-type: none"> 0 = read-only group (default) 1 = read-write group 2 = trap group <p>Note: all groups can be used to send traps.</p> |

5.11 Status & Diagnostics

The **Status & Diagnostics** menu is used to view and monitor the gateway's channels, Syslog messages, hardware and software product information, and to assess the gateway's statistics and IP connectivity information.

5.11.1 Gateway Statistics

The 'Gateway Statistics' screens under the Gateway Statistics menu is used to monitor real-time activity such as IP connectivity information, call details and call statistics, including the number of call attempts, failed calls, fax calls, etc.



Note: The 'Gateway Statistics' screens don't refresh automatically. To view updated information, re-access the required screen.

5.11.1.1 IP Connectivity

The 'IP Connectivity' screen provides you with online, read-only network diagnostic connectivity information on all destination IP addresses configured in the 'Tel to IP Routing' screen (refer to 'Tel to IP Routing Table' on page [134](#)).



Notes:

- This information is available only if the parameter AltRoutingTel2IPEnable (described in the table below) is set to 1 (Enable) or 2 (Status Only).
- The information in columns 'Quality Status' and 'Quality Info.' (per IP address) is reset if two minutes elapse without a call to that destination.

- **To view the IP connectivity information, take these 2 steps:**
1. Set the parameter 'Enable Alt Routing Tel to IP' (or *ini* file parameter AltRoutingTel2IPEnable) to Enable **[1]** or Status Only **[2]**. To configure this parameter, refer to 'General Parameters' on page 132.
 2. Open the 'IP Connectivity' screen (**Status & Diagnostics** menu > **Gateway Statistics** submenu > **IP Connectivity**).

Figure 5-60: IP Connectivity Screen

| IP Connectivity | | | | | | | |
|-----------------|-------------|---------------------|---------------------|----------------|---------------|----------------|----------------|
| IP Address | Host Name | Connectivity Method | Connectivity Status | Quality Status | Quality Info. | | DNS Status |
| 1 10.13.77.7 | 10.13.77.7 | Ping | CON_OK | QOS_UNKNOWN | PL[percent]:0 | DELAY [msec]:0 | DNS_DISABLE |
| 2 10.13.77.9 | 10.13.77.9 | Ping | CON_OK | QOS_UNKNOWN | PL[percent]:0 | DELAY [msec]:0 | DNS_DISABLE |
| 3 10.13.77.18 | 10.13.77.18 | Ping | CON_FAIL | QOS_UNKNOWN | PL[percent]:0 | DELAY [msec]:0 | DNS_DISABLE |
| 4 1.2.3.4 | doron_pc | Ping | CON_FAIL | QOS_UNKNOWN | PL[percent]:0 | DELAY [msec]:0 | DNS_RESOLVED |
| 5 10.13.2.95 | xyz | Ping | CON_INIT | QOS_UNKNOWN | PL[percent]:0 | DELAY [msec]:0 | DNS_UNRESOLVED |
| 6 UNUSED ENTRY | --- | --- | --- | --- | --- | --- | --- |
| 7 UNUSED ENTRY | --- | --- | --- | --- | --- | --- | --- |

Table 5-56: IP Connectivity Parameters

| Column Name | Description |
|----------------------------|--|
| IP Address | The IP address can be one of the following: <ul style="list-style-type: none"> IP address defined in the destination 'IP Address' field in the Tel to IP Routing table. IP address that is resolved from the host name defined in the 'Destination IP Address' field in the Tel to IP Routing table. |
| Host Name | Host name (or IP address) defined in the 'Destination IP Address' field in the Tel to IP Routing table. |
| Connectivity Method | The method according to which the destination IP address is queried periodically (currently only by ping). |
| Connectivity Status | Displays the status of the IP address' connectivity according to the method in the 'Connectivity Method' field. Can be one of the following: <ul style="list-style-type: none"> OK = Remote side responds to periodic connectivity queries. Lost = Remote side didn't respond for a short period. Fail = Remote side doesn't respond. Init = Connectivity queries not started (e.g., IP address not resolved). Disable = The connectivity option is disabled (AltRoutingTel2IPMode equals 0 or 2). |

Table 5-56: IP Connectivity Parameters

| Column Name | Description |
|-----------------------|--|
| Quality Status | <p>Determines the QoS (according to packet loss and delay) of the IP address. Can be one of the following:</p> <ul style="list-style-type: none">▪ Unknown = Recent quality information isn't available.▪ OK▪ Poor <p>Notes:</p> <ul style="list-style-type: none">▪ This field is applicable only if the parameter AltRoutingTel2IPMode is set to 2 or 3.▪ This field is reset if no QoS information is received for 2 minutes. |
| Quality Info. | <p>Displays QoS information: delay and packet loss, calculated according to previous calls.</p> <p>Notes:</p> <ul style="list-style-type: none">▪ This field is applicable only if the parameter AltRoutingTel2IPMode is set to 2 or 3.▪ This field is reset if no QoS information is received for 2 minutes. |
| DNS Status | <p>DNS status can be one of the following:</p> <ul style="list-style-type: none">▪ DNS Disable▪ DNS Resolved▪ DNS Unresolved |

5.11.1.2 Call Counters

The call counters screens include the 'IP to Tel Calls Count' and 'Tel to IP Calls Count' screens. These screens provide you with statistic information on incoming (IP→Tel) and outgoing (Tel→IP) calls. The statistic information is updated according to the release reason that is received after a call is terminated (during the same time as the end-of-call Call Detail Record or CDR message is sent). The release reason can be viewed in the 'Termination Reason' field in the CDR message. For detailed information on each counter, refer to the table below.

You can reset this information (refresh the display) by clicking the **Reset Counters** button.

➤ **To view the IP→Tel and Tel→IP Call Counters information, take this step:**

- Open the Call Counters screen you want to view (**Status & Diagnostics** menu > **Gateway Statistics** submenu > **IP to Tel Calls Count** or **Tel to IP Calls Count** option); the relevant Call Counters screen is displayed. The figure below shows the 'IP to Tel Calls Count' screen.

Figure 5-61: Calls Count Screen (e.g., Tel to IP)

| IP to Tel Calls Count | |
|---|-----------|
| Number of Attempted Calls | 53 |
| Number of Established Calls | 36 |
| Percentage of Successful Calls(ASR) | 67.924528 |
| Number of Calls Terminated due to a Busy Line | 4 |
| Number of Calls Terminated due to No Answer | 13 |
| Number of Calls Terminated due to Forward | 0 |
| Number of Failed Calls due to No Route | 0 |
| Number of Failed Calls due to No Matched Capabilities | 0 |
| Number of Failed Calls due to No Resources | 0 |
| Number of Failed Calls due to Other Failures | 0 |
| Average Call Duration(ACD)[sec] | 0 |
| Attempted Fax Calls Counter | 0 |
| Successful Fax Calls Counter | 0 |

Table 5-57: Call Counters Description

| Counter | Description |
|----------------------------------|--|
| Number of Attempted Calls | Indicates the number of attempted calls. It is composed of established and failed calls. The number of established calls is represented by the 'Number of Established Calls' counter. The number of failed calls is represented by the five failed-call counters. Only one of the established / failed call counters is incremented every time. |

Table 5-57: Call Counters Description

| Counter | Description |
|--|--|
| Number of Established Calls | <p>Indicates the number of established calls. It is incremented as a result of one of the following release reasons if the duration of the call is greater than zero:</p> <ul style="list-style-type: none"> GWAPP_REASON_NOT_RELEVANT (0) GWAPP_NORMAL_CALL_CLEAR (16) GWAPP_NORMAL_UNSPECIFIED (31) <p>And the internal reasons:</p> <ul style="list-style-type: none"> RELEASE_BECAUSE_UNKNOWN_REASON RELEASE_BECAUSE_REMOTE_CANCEL_CALL RELEASE_BECAUSE_MANUAL_DISC RELEASE_BECAUSE_SILENCE_DISC RELEASE_BECAUSE_DISCONNECT_CODE <p>Note: When the duration of the call is zero, the release reason GWAPP_NORMAL_CALL_CLEAR increments the 'Number of Failed Calls due to No Answer' counter. The rest of the release reasons increment the 'Number of Failed Calls due to Other Failures' counter.</p> |
| Percentage of Successful Calls (ASR) | The percentage of established calls from attempted calls. |
| Number of Calls Terminated due to a Busy Line | <p>Indicates the number of calls that failed as a result of a busy line. It is incremented as a result of the following release reason:</p> <p>GWAPP_USER_BUSY (17)</p> |
| Number of Calls Terminated due to No Answer | <p>Indicates the number of calls that weren't answered. It's incremented as a result of one of the following release reasons:</p> <ul style="list-style-type: none"> GWAPP_NO_USER_RESPONDING (18) GWAPP_NO_ANSWER_FROM_USER_ALERTED (19) <p>And (when the call duration is zero) as a result of the following:</p> <p>GWAPP_NORMAL_CALL_CLEAR (16)</p> |
| Number of Calls Terminated due to Forward | <p>Indicates the number of calls that were terminated due to a call forward. The counter is incremented as a result of the following release reason:</p> <p>RELEASE_BECAUSE_FORWARD</p> |
| Number of Failed Calls due to No Route | <p>Indicates the number of calls whose destinations weren't found. It is incremented as a result of one of the following release reasons:</p> <ul style="list-style-type: none"> GWAPP_UNASSIGNED_NUMBER (1) GWAPP_NO_ROUTE_TO_DESTINATION (3) |
| Number of Failed Calls due to No Matched Capabilities | <p>Indicates the number of calls that failed due to mismatched gateway capabilities. It is incremented as a result of an internal identification of capability mismatch. This mismatch is reflected to CDR via the value of the parameter DefaultReleaseReason (default is GWAPP_NO_ROUTE_TO_DESTINATION (3)), or by the GWAPP_SERVICE_NOT_IMPLEMENTED_UNSPECIFIED(79) reason.</p> |

Table 5-57: Call Counters Description

| Counter | Description |
|---|---|
| Number of Failed Calls due to No Resources | Indicates the number of calls that failed due to unavailable resources or a gateway lock. The counter is incremented as a result of one of the following release reasons: <ul style="list-style-type: none"> GWAPP_RESOURCE_UNAVAILABLE_UNSPECIFIED RELEASE_BECAUSE_GW_LOCKED |
| Number of Failed Calls due to Other Failures | This counter is incremented as a result of calls that fail due to reasons not covered by the other counters. |
| Average Call Duration (ACD) [sec] | The average call duration of established calls. |
| Attempted Fax Calls Counter | Indicates the number of attempted fax calls. |
| Successful Fax Calls Counter | Indicates the number of successful fax calls. |

5.11.1.3 Call Routing Status

The 'Call Routing Status' screen provides you with information on the current routing method used by the gateway. This information includes the IP address and FQDN (if used) of the Proxy server with which the gateway currently operates.

- **To view the 'Call Routing Status' screen, take this step:**
 - Open the 'Call Routing Status' screen (**Status & Diagnostics** menu > **Gateway Statistics** submenu > **Calls Routing Status** option).

Figure 5-62: Call Routing Status Screen

| Call Routing Status | |
|-----------------------------|---------------|
| Current Call-Routing Method | Routing Table |
| Current Proxy | Not Used (--) |
| Current Proxy State | -- |

Table 5-58: Call Routing Status Parameters

| Parameter | Description |
|------------------------------------|---|
| Current Call-Routing Method | <ul style="list-style-type: none"> Proxy = Proxy server is used to route calls. Routing Table preferred to Proxy = The Tel to IP Routing table takes precedence over a Proxy for routing calls (PreferRouteTable = 1). Routing Table = The Tel to IP Routing table is used to route calls. |

Table 5-58: Call Routing Status Parameters

| Parameter | Description |
|----------------------------|---|
| Current Proxy | <ul style="list-style-type: none"> Not Used = Proxy server isn't defined. IP address and FQDN (if exists) of the Proxy server the gateway currently operates with. |
| Current Proxy State | <ul style="list-style-type: none"> N/A = Proxy server isn't defined. OK = Communication with the Proxy server is in order. Fail = No response from any of the defined Proxies. |

5.11.1.4 SAS Registered Users

The 'SAS Registered Users' screen provides you with a list of up to 100 SAS Registered Users.

➤ **To view the 'SAS Registered Users' screen, take this step:**

- Open the 'SAS Registered Users' screen (**Status & Diagnostics** menu > **Gateway Statistics** submenu > **SAS Registered Users** option).

Figure 5-63: SAS Registered Users Screen

| SAS Registered Users | |
|-----------------------|-----------------------------------|
| Address Of Record | Contact |
| <sip:2400@Proxies.ac> | <sip:2400@10.8.210.5>;expires=180 |
| <sip:2401@Proxies.ac> | <sip:2401@10.8.210.5>;expires=180 |
| <sip:2500@Proxies.ac> | <sip:2500@10.8.210.5>;expires=180 |
| <sip:2402@Proxies.ac> | <sip:2402@10.8.210.5>;expires=180 |
| <sip:2403@Proxies.ac> | <sip:2403@10.8.210.5>;expires=180 |
| <sip:2404@Proxies.ac> | <sip:2404@10.8.210.5>;expires=180 |
| <sip:2405@Proxies.ac> | <sip:2405@10.8.210.5>;expires=180 |

Table 5-59: SAS Registered Users Parameters

| Column Name | Description |
|--------------------------|--|
| Address of Record | An address-of-record (AOR) is a SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI (Contact) where the user might be available. |
| Contact | SIP URI that can be used to contact that specific instance of the UA for subsequent requests. |

5.11.2 Activating the Internal Syslog Viewer

The 'Message Log' screen displays Syslog debug messages sent by the gateway. You can simply select the messages, and then copy and paste them into a text editor such as Notepad. This text file (*txt*) can then be sent to AudioCodes Technical Support for diagnosis and troubleshooting.



Note: It's not recommended to keep a Message Log session open (even if the window is minimized), for a prolonged period. This may cause the gateway to overload. For prolong debugging use an external Syslog server (refer to the *SIP Series Reference Manual*).

➤ To activate the Message Log, take these 3 steps:

1. In the 'General Parameters' screen (**Protocol Management** menu > **Advanced Parameters** submenu > **General Parameters** option), set the parameter 'Debug Level' (or *ini* file parameter GwDebugLevel) to 5 (refer to 'General Parameters' on page 103). This parameter determines the Syslog logging level in the range 0 to 5, where 5 is the highest level.
2. Open the 'Message Log' screen (**Status & Diagnostics** menu > **Message Log**); the 'Message Log' screen is displayed and the log is activated.

Figure 5-64: Message Log Screen

```
Log is Activated

12d:6h:56m:26s (    lgr_flow) (460      ) ---- Incoming SIP Message from 10.8.58.1:5060 ----

12d:6h:56m:26s INVITE sip:200@10.8.58.4:user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.58.1;branch=z9hG4bKackpUGBoT
Max-Forwards: 70
From: <sip:100@10.8.58.1>;tag=1c910315947
To: <sip:200@10.8.58.4:user=phone>
Call-ID: 1254421147LEqU@10.8.58.1
CSeq: 1 INVITE
Contact: <sip:100@10.8.58.1>
Supported: em, timer, replaces, path
Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, UPDATE
User-Agent: Audiocodes-Sip-Gateway-MP-104 FXS/v.4.40.123.223
Content-Type: application/sdp
Content-Length: 161
```

3. To clear the screen of messages, click the submenu **Message Log** again; the screen is cleared and new messages begin appearing.

➤ To de-activate the Message Log, take this step:

- Close the screen by accessing any another screen.

5.11.3 Device Information

The 'Device Information' screen displays the gateway's specific hardware and software product information. This information can help you to expedite troubleshooting. Capture the screen and email it to AudioCodes Technical Support personnel to ensure quick diagnosis and effective corrective action. From this screen you can also view and remove any loaded files used by the gateway (stored in the RAM).

➤ **To access the 'Device Information' screen, take this step:**

- Open the 'Device Information' screen (**Status & Diagnostics** menu > **Device Information**).

| Device Information | |
|------------------------------|------------------------|
| General | |
| MAC Address: | 00908f09f34b |
| Serial Number: | 652107 |
| Board Type: | 47 |
| Device Up Time: | 0d:0h:2m:45s:0th |
| Device Administrative State: | Unlocked |
| Device Operational State: | Disabled |
| Flash Size [bytes]: | 33554432 |
| RAM Size [bytes]: | 134217728 |
| CPU Speed [MHz]: | 200 |
| Versions | |
| Version ID: | 5.20A.000.006 |
| DSP Type: | 2 |
| DSP Software Version: | 52006 |
| DSP Software Name: | 624AE3 |
| Flash Version: | 206 |
| Loaded Files | |
| Loaded Call Progress Tones: | Default Progress Tones |
| Loaded Coder Table : | Default CODERTABLE |

➤ **To delete any of the loaded files, take this step:**

- Click the **Delete** button to the right of the files you want to delete. Deleting a file takes effect only after the gateway is reset (refer to 'Resetting the Gateway' on page 279).

5.11.4 Viewing the Ethernet Port Information

The 'Ethernet Port Information' screen provides read-only information on the Ethernet connection used by the gateway. For detailed information on the Ethernet redundancy scheme, refer to 'Ethernet Interface Redundancy' on page 423. For detailed information on the Ethernet interface configuration, refer to 'Ethernet Interface Configuration' on page 423.

➤ **To view the Ethernet Port Information parameters, take the following step:**

- Open the 'Ethernet Port Information' screen (**Status & Diagnostics** menu > **Ethernet Port Information** submenu).

| Ethernet Port Information | |
|---------------------------|---------------|
| Active Port | 1 |
| Port 1 Duplex Mode | Half Duplex |
| Port 1 Speed | 100 Mbps |
| Port 2 Duplex Mode | Not Available |
| Port 2 Speed | Not Available |

Table 5-60: Ethernet Port Information Parameters

| Parameter | Description |
|--------------------|---|
| Active Port | Displays the active Ethernet port (1 or 2). |
| Port 1 Duplex Mode | Displays the Duplex mode Ethernet port 1 is using (Half Duplex or Full Duplex). |
| Port 1 Speed | Displays the speed (in Mbps) that Ethernet port 1 is using (10 Mbps; 100 Mbps). |
| Port 2 Duplex Mode | Displays the Duplex mode Ethernet port 2 is using (Half Duplex or Full Duplex). |
| Port 2 Speed | Displays the speed (in Mbps) that Ethernet port 2 is using (10 Mbps; 100 Mbps). |

5.11.5 Viewing Performance Statistics

The Performance Statistic submenu provides read-only, gateway performance statistics. This menu includes the Basic Statistic, Control Protocol Statistics, Networking Statistics, DS1 Trunk Statistics, DSP Statistics screen.

- **To view performance statistics, take the following step:**
 - Open the 'Basic Statistics' screen (**Status & Diagnostics** menu > **Performance Statistics** submenu).

Figure 5-65: Basic Statistics Screen

| Basic Statistics | |
|---------------------------|---------|
| Active TDM channels | 0 |
| Active DSP resources | 1 |
| Active analog channels | 0 |
| Active G.711 channels | 1 |
| Average voice delay (ms) | 2 |
| Average voice jitter (ms) | 4 |
| Total RTP packets TX | 2554981 |
| Total RTP packets RX | 19862 |

- **To reset the performance statistics of a specific screen to zero, take the following step:**
 - Click the **Reset Statistics** button.

5.12 Software Update

The Software Update menu enables users to upgrade the gateway software by loading a new *cmp* file along with the *ini* file and a suite of auxiliary files, or to update the existing auxiliary files.

The Software Update menu includes the following submenus:

- Software Upgrade Wizard (refer to 'Software Upgrade Wizard' on page 262)
- Load Auxiliary Files (refer to 'Auxiliary Files' on page 269)
- Software Upgrade Key (refer to Updating the Software Upgrade Key on page 271)



Note: When upgrading the gateway software, you *must* load the new *cmp* file with all other related configuration files.

5.12.1 Software Upgrade Wizard

The Software Upgrade Wizard guides you through the process of software upgrade: selecting files and loading them to the gateway. The wizard also enables you to upgrade software while maintaining the existing configuration. Using the wizard obligates you to load and burn a *cmp* file to the gateway. You can choose to also use the wizard to load the *ini* and auxiliary files (e.g., Call Progress Tones), but this option cannot be pursued without loading the *cmp* file. For the *ini* and each auxiliary file type, you can choose to reload an existing file, load a new file, or not load a file at all.

The Software Upgrade Wizard allows you to load the following files:

- *cmp* (mandatory)
- *ini*
- Auxiliary files:
 - CPT (Call Progress Tone)
 - VP (Voice Prompts)
 - PRT (Prerecorded Tones)
 - CAS
 - FXS
 - FXO
 - USRINF (User Info)



Warning: The Software Upgrade Wizard requires the gateway to be reset at the end of the process, which may disrupt its traffic. To avoid this, disable all traffic on the device before initiating the wizard by performing a graceful lock (refer to 'Locking and Unlocking the Gateway' on page 276).

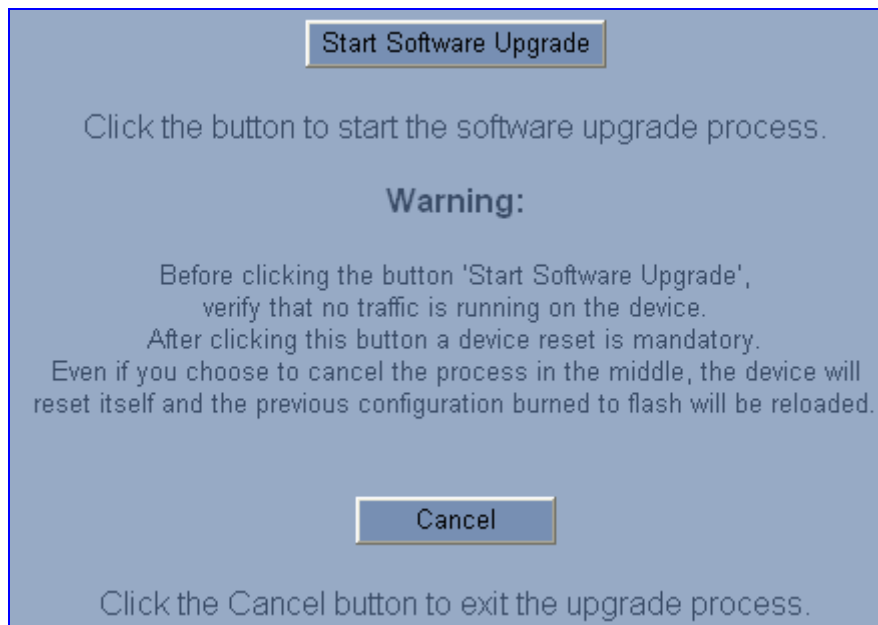
**Notes:**

- When you activate the wizard, the rest of the Embedded Web Server interface is unavailable and the background Web screen is disabled. After the process is completed, access to the full Embedded Web Server is restored.
- The wizard allows you to load an *ini* or auxiliary file only after you have loaded a CMP file.

➤ **To use the Software Upgrade Wizard, take these 10 steps:**

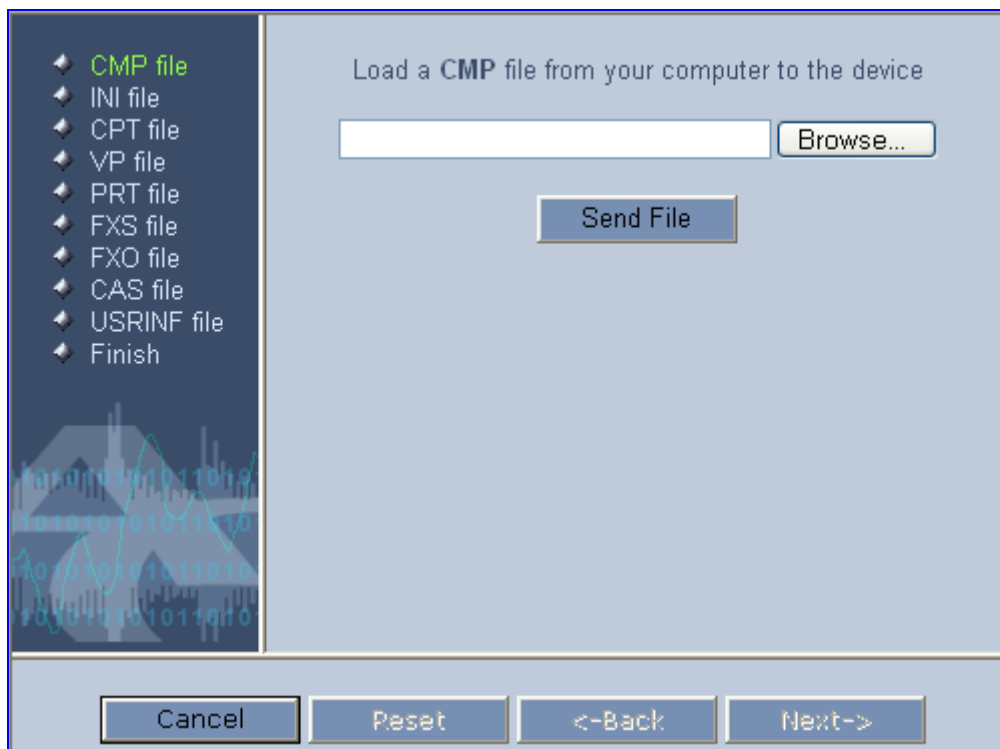
1. Stop all traffic on the gateway (refer to the note above).
2. Open the 'Software Upgrade Wizard' (**Software Update** menu > **Software Upgrade Wizard**); the 'Start Software Upgrade' screen appears.

Figure 5-66: Start Software Upgrade Wizard Screen



Note: At this stage, the Software Upgrade Wizard can be canceled (by clicking **Cancel**), without requiring a gateway reset. However, if you continue the wizard (by clicking the **Start Software Upgrade** button), the process must be followed through and completed with a gateway reset. If you click the **Cancel** button in any of the subsequent screens, the gateway is automatically reset with the configuration that was previously burned in flash memory.

3. Click the **Start Software Upgrade** button; the 'Load a cmp file' screen appears.



4. Click the **Browse** button, navigate to the *cmp* file, and then click **Send File**; the *cmp* file is loaded to the gateway and you're notified as to a successful loading, as shown below.



5. Note that the four action buttons (**Cancel**, **Reset**, **Back**, and **Next**) are now activated (following *cmp* file loading). You can now choose to either:

- Click **Reset**; the gateway resets, utilizing the new *cmp* you loaded and utilizing the current configuration files.
- Click **Cancel**; the gateway resets utilizing the *cmp*, *ini* and all other configuration files that were previously stored in flash memory. Note that these are NOT the files you loaded in the previous wizard steps.
- Click **Back**; the 'Load a *cmp* File' screen is displayed again.
- Click **Next**; the 'Load an *ini* File' screen opens; refer to the figure below. Loading a new *ini* file or any other auxiliary file listed in the wizard is optional.

Note that as you progress, the file type list on the left indicates which file type loading is in process by illuminating green (until 'Finish').

6. In the 'Load an *ini* File' screen, you can now choose to either:

- Click **Browse** and navigate to the *ini* file; the check box 'Use existing configuration', by default checked, becomes unchecked. Click **Send File**; the *ini* file is loaded to the gateway and you're notified as to a successful loading.
- Ignore the **Browse** button (its field remains undefined and the check box 'Use existing configuration' remains checked by default).
- Ignore the **Browse** button and uncheck the 'Use existing configuration' check box; no *ini* file is loaded, the gateway uses its factory-preconfigured values.

7. You can now choose to either:

- Click **Cancel**; the gateway resets utilizing the *cmp*, *ini* and all other configuration files that were previously stored in flash memory. Note that these are NOT the files you loaded in the previous Wizard steps.
- Click **Reset**; the gateway resets, utilizing the new *cmp* and *ini* file you loaded up to now as well as utilizing the other configuration files.
- Click **Back**; the 'Load a *cmp* file' screen is reverted to.
- Click **Next**; the next screen opens for loading a specific auxiliary file listed in the Wizard.

8. Follow the same procedure as for loading the *ini* file (Step 6) for loading the auxiliary files.

9. In the 'FINISH' screen (refer to the figure below), the **Next** button is disabled. Complete the upgrade process by clicking **Reset** or **Cancel**.

- Click **Reset**, the gateway 'burns' the newly loaded files to flash memory and then resets the gateway. After the gateway resets, the 'End Process' screen appears displaying the burned configuration files (refer to the figure below).

- Click **Cancel**, the gateway resets, utilizing the files previously stored in flash memory. (Note that these are NOT the files you loaded in the previous wizard steps).

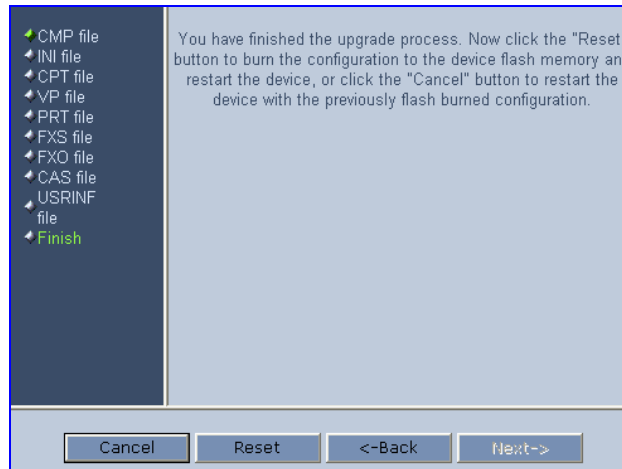
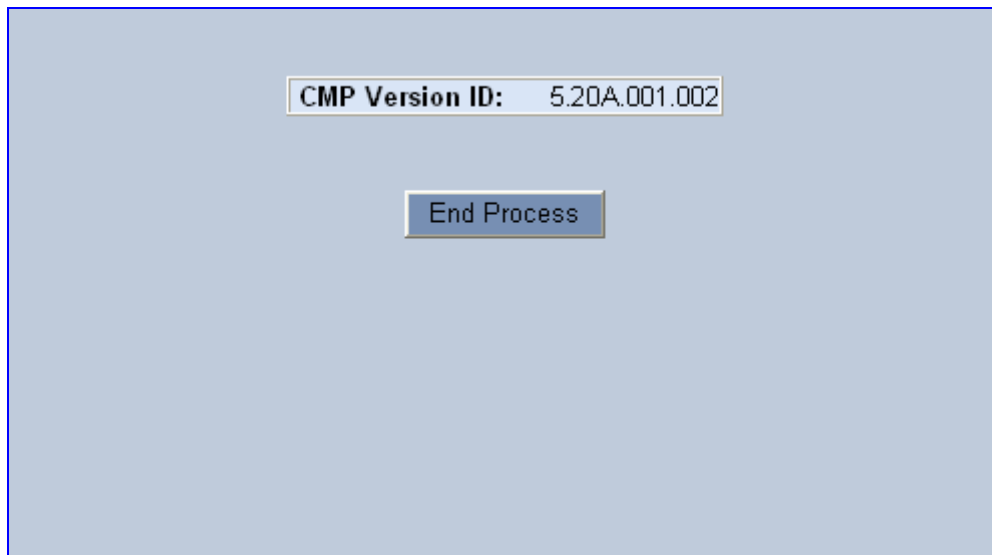


Figure 5-67: End Process Wizard Screen



- Click the **End Process** button; the 'Enter Network Password' screen appears requesting login username and password (described in 'Accessing the Embedded Web Server' on page 60). Once logged in, the Embedded Web Server reflects the upgraded gateway.

5.12.2 Automatic Update Mechanism

The gateway can automatically update its *cmp*, *ini*, and configuration files. These files can be stored on any standard Web, FTP, or NFS server and can be loaded periodically to the gateway via HTTP, HTTPS, FTP, or NFS. This mechanism can be used even for gateways that are installed behind NAT and firewalls.

The Automatic Update mechanism is applied separately to each file. For a detailed list of available files and their corresponding parameters, refer to 'System Parameters' on page 308.



Note: The Automatic Update mechanism assumes the external Web server conforms to the HTTP standard. If the Web server ignores the If-Modified-Since header, or doesn't provide the current date and time during the HTTP 200 OK response, the gateway may reset itself repeatedly. To overcome this problem, adjust the update frequency (AutoUpdateFrequency).

The following methods are used to activate the Automatic Update mechanism:

- After the gateway starts up (refer to the Startup process described in 'Startup Process' on page 48).
- At a configurable time of day (e.g., 18:00) using the *ini* file parameter AutoUpdatePredefinedTime. This option is disabled by default.
- At fixed intervals (e.g., every 60 minutes) using the *ini* file parameter AutoUpdateFrequency. This option is disabled by default.

The following *ini* file example can be used to activate the Automatic Update mechanism.

```
# DNS is required for specifying domain names in URLs
DnsPriServerIP = 10.1.1.11
# Load an extra configuration ini file using HTTP
IniFileURL = 'http://webserver.corp.com/AudioCodes/inifile.ini'
# Load Call Progress Tones file using HTTPS
CptFileUrl = 'https://10.31.2.17/usa tones.dat'
# Load Voice Prompts file using FTPS with user 'root' and password 'wheel'
VPFileUrl = 'ftps://root:wheel@ftpserver.corp.com/vp.dat'
# Update every day at 03:00 AM
AutoUpdatePredefinedTime = '03:00'
# Note: The cmp file isn't updated since it's disabled by default
(AutoUpdateCmpFile) .
```

Note the following:

- When HTTP or HTTPS are used, the gateway queries the Web server/s for the requested files. The *ini* file is loaded only if it was modified since the last automatic update. The *cmp* file is loaded only if its version is different from the version stored on the gateway's non-volatile memory. All other auxiliary files (e.g., CPT) are updated only once. To update a previously loaded auxiliary file, you must update the parameter containing its URL.
- To load different configurations (*ini* files) for specific gateways, add the string '<MAC>' to the URL. This mnemonic is replaced with the gateway's hardware MAC address, resulting in an *ini* file name request that contains the gateway's MAC address.
- To automatically update the *cmp* file, use the parameter CmpFileURL to specify its name and location. As a precaution (to protect the gateway from an accidental update), by default, the Automatic Update mechanism doesn't apply to the *cmp* file. Therefore, (to enable it) set the parameter AutoUpdateCmpFile to 1.

The following example illustrates how to utilize Automatic Updates for deploying gateway with minimum manual configuration.

➤ **To utilize Automatic Updates for deploying the gateway with minimum manual configuration, take these 5 steps:**

1. Setup a Web server (e.g., <http://www.corp.com>) where all configuration files are located.
2. For each gateway, pre-configure the following parameter (DHCP / DNS are assumed):
IniFileURL = 'http://www.corp.com/master_configuration.ini'
3. Create a file named *master_configuration.ini* with the following text:

```
# Common configuration for all devices
# -----
CptFileURL = 'http://www.corp.com/call progress.dat'
# Check for updates every 60 minutes
AutoUpdateFrequency = 60

# Additional configuration per device
# -----
# Each device loads a file named after its MAC address,
# (e.g., config 00908F033512.ini)
IniFileURL = 'http://www.corp.com/config <MAC>.ini'

# Reset the device after configuration is updated.
# The device resets after all of the files are processed.
```

You can modify the *master_configuration.ini* file (or any of the *config_<MAC>.ini* files) at any time. The gateway queries for the latest version every 60 minutes and applies the new settings immediately.

4. For additional security, use HTTPS or FTPS. The gateway supports HTTPS (RFC 2818) and FTPS using the AUTH TLS method <draft-murray-auth-ftp-ssl-16> for the Automatic Update mechanism.
5. To load configuration files from an NFS server, the NFS file system parameters should be defined in the configuration *ini* file. The following is an example of an *ini* file for loading files from NFS servers using NFS version 2.

```
# Define NFS servers for Automatic Update
[ NFSServers ]
FORMAT NFSServers_Index = NFSServers_HostOrIP,
NFSServers_RootPath, NFSServers_NfsVersion;
NFSServers 1 = 10.31.2.10, /usr/share, 2 ;
NFSServers 2 = 192.168.100.7, /d/shared, 2 ;
[ \NFSServers ]
CptFileUrl = 'file://10.31.2.10/usr/share/public/usa tones.dat'
VpFileUrl =
'file://192.168.100.7/d/shared/audiocodes/voiceprompt.dat'
```

5.12.3 Auxiliary Files

The 'Auxiliary Files' screen enables you to load various auxiliary files to the gateway, as described in the table below. (For detailed information on these files, refer to the *SIP Series Reference Manual*). For information on deleting these files from the gateway, refer to 'Device Information' on page 259.

Table 5-61: Auxiliary Files Descriptions

| File Type | Description |
|---------------------|--|
| Coefficient | This file (different file for FXS and FXO modules) contains the telephony interface configuration information for the VoIP gateway. This information includes telephony interface characteristics such as DC and AC impedance, feeding current, and ringing voltage. This file is specific to the type of telephony interface that the VoIP gateway supports. In most cases, you are required to load this type of file. |
| CAS | Up to 8 different CAS files containing specific CAS protocol definitions for digital modules. These files are provided to support various types of CAS signaling. |
| Voice Prompts | The voice announcement file contains a set of Voice Prompts (VP) to be played by the gateway during operation. |
| Dial Plan | Dial plan file. |
| Call Progress Tones | This is a region-specific, telephone exchange-dependent file that contains the Call Progress Tones levels and frequencies that the VoIP gateway uses. The default CPT file is: U.S.A. |
| Prerecorded Tones | The <i>.dat</i> PRT file enhances the gateway's capabilities of playing a wide range of telephone exchange tones that cannot be defined in the Call Progress Tones file. |
| User Info | The User Information file maps PBX extensions to IP numbers. This file can be used to represent PBX extensions as IP phones in the global 'IP world'. |

5.12.3.1 Loading the Auxiliary Files via the Embedded Web Server

- To load an auxiliary file to the gateway using the Embedded Web Server, take these 8 steps:

1. Open the 'Auxiliary Files' screen (**Software Update** menu > **Load Auxiliary Files**).

Figure 5-68: Auxiliary Files Screen



Auxiliary Files

Send FXS "Coefficient" file from your computer to the device

Send FXO "Coefficient" file from your computer to the device

Send "CAS" file from your computer to the device

Send "Voice Prompts" file from your computer to the device

Send "Call Progress Tones" file from your computer to the device

Send "Prerecorded Tones" file from your computer to the device

Send "User Info" file from your computer to the device

2. Click the **Browse** button corresponding to the type of file that you want to load.
3. Navigate to the folder that contains the file you want to load.
4. Select the file, and then click **Open**; the name and path of the file appear in the field next to the **Browse** button.
5. Click the **Send File** button corresponding to the field that contains the name of the file you want to load.
6. Repeat steps 2 through 5 for each file you want to load.
7. To save the loaded auxiliary files to flash memory, refer to 'Saving Configuration' on page 278.
8. To reset the gateway, refer to 'Resetting the Gateway' on page 279.

**Notes:**

- Saving an auxiliary file to flash memory may disrupt traffic on the gateway. To avoid this, disable all traffic on the device by performing a graceful lock (refer to 'Locking and Unlocking the Gateway' on page 276).
- File names preceded by an exclamation mark (!) are not changeable on-the-fly and require that the device be reset (e.g., Call Progress Tones file).

5.12.3.2 Loading the Auxiliary Files via the ini File

Before you load the auxiliary files (Call Progress Tones, Prerecorded Tones, User Information, Voice Prompts, Dial Plan, FXS/FXO Coefficient, and CAS) to the gateway, in the *ini* file you need to define certain *ini* file parameters associated with these files. These *ini* file parameters specify the files that you want loaded and whether they must be stored in the non-volatile memory.

For a description of the *ini* file parameters associated with the auxiliary files, refer to 'Configuration Files Parameters' on page 378.

➤ **To load the auxiliary files via the *ini* file, take these 3 steps:**

1. In the *ini* file, define the auxiliary files to be loaded to the gateway. You can also define in the *ini* file whether the loaded files must be stored in the non-volatile memory so that the TFTP process is not required every time the gateway boots up.
2. Save the auxiliary files you want to load and the *ini* file in the same directory on your PC.
3. Invoke a BootP/TFTP session; the *ini* and auxiliary files are loaded to the gateway.

5.12.4 Updating the Software Upgrade Key

The gateways are supplied with a Software Upgrade Key. You can later upgrade the gateway features, capabilities, and quantity of available resources by specifying what upgrades are required, and by purchasing a new key to match your requirements.

The Software Upgrade Key is provided in string format in a text file, which is loaded to the gateway. Stored in the gateway's non-volatile flash memory, the string defines the features and capabilities allowed by the specific key that is purchased. The gateway uses *only* these features and capabilities. A new key overwrites a previously installed key.

**Notes:**

- The Software Upgrade Key is an encrypted key.
- The Software Upgrade Key is provided only by AudioCodes.

5.12.4.1 Backing up the Current Software Upgrade Key

Backup your current Software Upgrade Key before loading a new key to the device. You can always re-load this backed-up key (refer to 'Loading the Software Upgrade Key' on page 272) to restore your device capabilities to what they originally were if the new key doesn't comply with your requirements.

➤ **To backup the current Software Upgrade Key, take these 5 steps:**

1. Access the devices Embedded Web Server (refer to 'Accessing the Embedded Web Server' on page 60).
2. Click the **Software Update** button.
3. Click the **Software Upgrade Key** tab; the Software Upgrade Key screen is displayed (shown in 'Using the Embedded Web Server' on page 273).
4. Copy the string of text from the 'Current Key' text box and paste it in a new text file.
5. Save the text file on your PC with a name of your choosing.

5.12.4.2 Loading the Software Upgrade Key

After receiving the Software Upgrade Key file, ensure that the first line displays "[LicenseKeys]" and that it contains one or more lines in the following format:

S/N<Serial Number of TPM> = <long Software Upgrade Key>

For example: S/N370604 = jCx6r5tovCIKaBBbhPtT53Yj...

One S/N must match the S/N of your device. The device's S/N can be viewed in the 'Device Information' screen (refer to 'Device Information' on page 259).



Warning: Don't modify the contents of the Software Upgrade Key file.

You can load a Software Upgrade Key using one of the following tools:

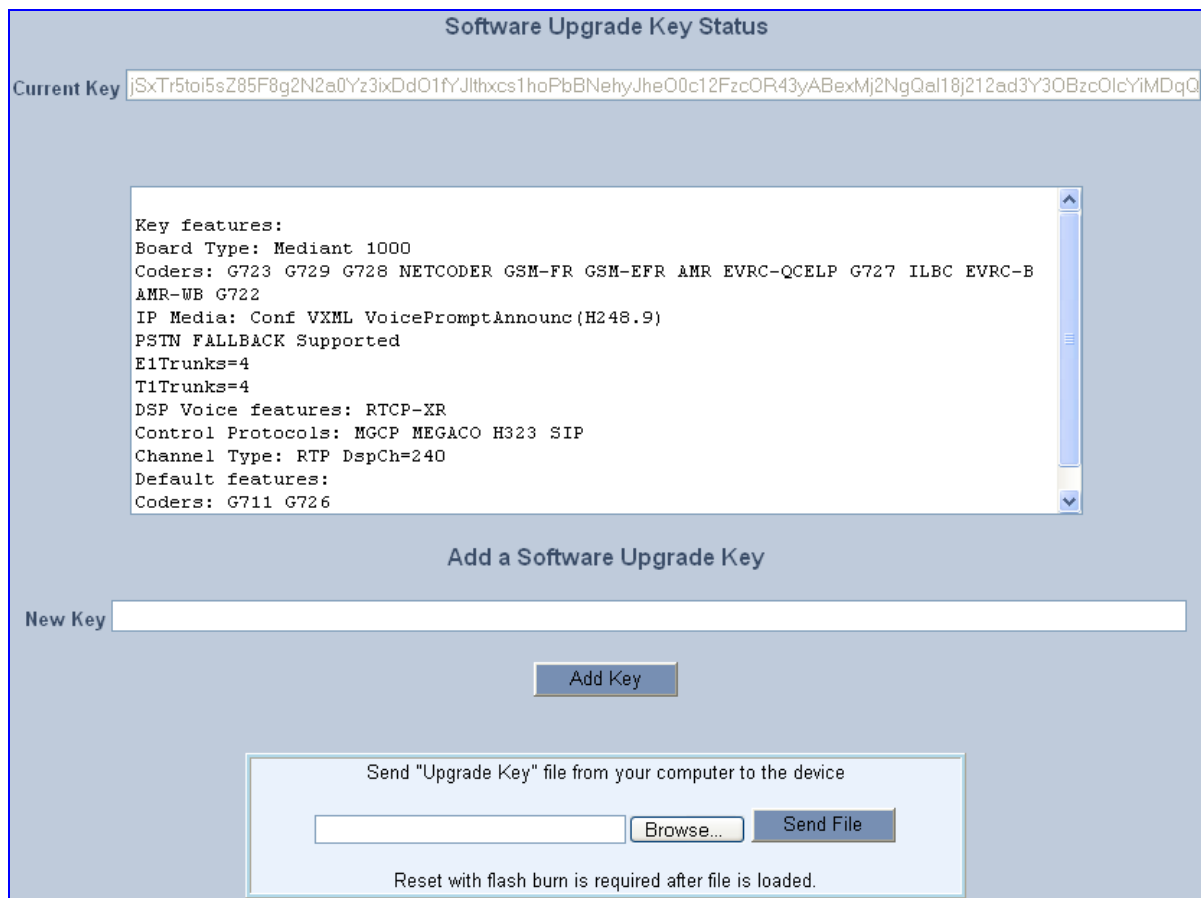
- Embedded Web Server (refer to 'Using the Embedded Web Server' on page 273)
- BootP/TFTP configuration utility (refer to the *SIP Series Reference Manual*)
- AudioCodes' EMS (refer to *AudioCodes' EMS User's Manual* or *EMS Product Description*)

5.12.4.2.1 Using the Embedded Web Server

The procedure below describes how to load a Software Upgrade Key to the gateway using the Embedded Web Server.

➤ **To load a Software Upgrade Key using the Embedded Web Server, take these 5 steps:**

1. Access the device's Embedded Web Server (refer to 'Accessing the Embedded Web Server' on page 60).
2. Click the **Software Update** button.
3. Click the **Software Upgrade Key** tab; the 'Software Upgrade Key' screen is displayed (shown in the figure below).



Software Upgrade Key Status

Current Key

Key features:

Board Type: Mediant 1000

Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B

AMR-WB G722

IP Media: Conf VXML VoicePromptAnnounc (H248.9)

PSTN FALLBACK Supported

E1Trunks=4

T1Trunks=4

DSP Voice features: RTCP-XR

Control Protocols: MGCP MEGACO H323 SIP

Channel Type: RTP DspCh=240

Default features:

Coders: G711 G726

Add a Software Upgrade Key

New Key

Send "Upgrade Key" file from your computer to the device

Reset with flash burn is required after file is loaded.

- When loading a single key S/N line to a device:
 - a. Open the Software Upgrade Key file (using, for example, Microsoft® Notepad).
 - b. Select and copy the key string of the device's S/N and paste it into the field 'New Key'. If the string is sent in the body of an email, copy and paste it from there.
 - c. Click the **Add Key** button.

- When loading a Software Upgrade Key text file containing multiple S/N lines to a device (refer to the figure below):

Figure 5-69: Software Upgrade Key with Multiple S/N Lines



- Click the **Browse** button in the 'Send "Upgrade Key" file from your computer to the device' field, and navigate to the Software Upgrade Key text file.
 - Click the **Send File** button; the new key is loaded to the device and validated. If the key is valid, it's burned to memory. The new key is displayed in the 'Current Key' field.
- Verify the presence of the appropriate features of the new key, by scrolling through the 'Key features:' group.
 - After verifying that the Software Upgrade Key was successfully loaded, reset the device; the new capabilities and resources are active.

5.12.4.2.2 Using BootP/TFTP

The procedure below describes how to load a Software Upgrade Key to the gateway using AudioCodes' BootP/TFTP Server utility.

- **To load a Software Upgrade Key file using BootP/TFTP, take these 6 steps:**
 - Place the file in the same folder in which the gateway's *cmp* file is located. Note that to load the Software Upgrade Key via a TFTP server, the extension name of the key file must be *ini*.
 - Start the BootP/TFTP Server utility.
 - From the **Services** menu, choose **Clients**; the 'Client Configuration' screen is displayed (refer to the *SIP Series Reference Manual*).
 - From the 'INI File' drop-down list, select the Software Upgrade Key file. Note that the gateway's *cmp* file must be specified in the 'Boot File' field.
 - Configure the initial BootP/TFTP parameters as required (refer to the *SIP Series Reference Manual*), and then click **OK**.
 - Reset the gateway; the *cmp* and Software Upgrade Key files are loaded to the gateway.

5.12.4.3 Verifying that the Key was Successfully Loaded

You can verify if the Software Upgrade Key file has been successfully loaded to the gateway by using one of the following methods:

- In the Embedded Web Server's read-only 'Key features:' group (**Software Update** menu > **Software Upgrade Key**) (refer to 'Using the Embedded Web Server' on page 273), verify that the features and capabilities activated by the installed string match those that were ordered.
- Access the Syslog server (refer to the *SIP Series Reference Manual*) and ensure that the following message appears in the Syslog server: **'S/N___ Key Was Updated. The Board Needs to be Reloaded with ini file\n'**

5.12.4.4 Troubleshooting an Unsuccessful Loading of a Key

If the Syslog server indicates that a Software Upgrade Key file was unsuccessfully loaded (the SN_ line is blank), take the following preliminary actions to troubleshoot the issue:

- Open the Software Upgrade Key file and check that the S/N line of the specific gateway whose key you want to update is listed. If it isn't, contact AudioCodes.
- Verify that you've loaded the correct file and that you haven't loaded the gateway's *ini* file or the CPT *ini* file by mistake. Open the file and ensure that the first line displays "[LicenseKeys]".
- Verify that you didn't alter in any way the contents of the file.

5.13 Maintenance

The Maintenance menu is used for the following operations:

- Locking and unlocking the gateway (refer to 'Locking and Unlocking the Gateway' on page 276)
- Saving the gateway's configuration (refer to 'Saving Configuration' on page 278)
- Resetting the Gateway (refer to 'Resetting the Gateway' on page 279)

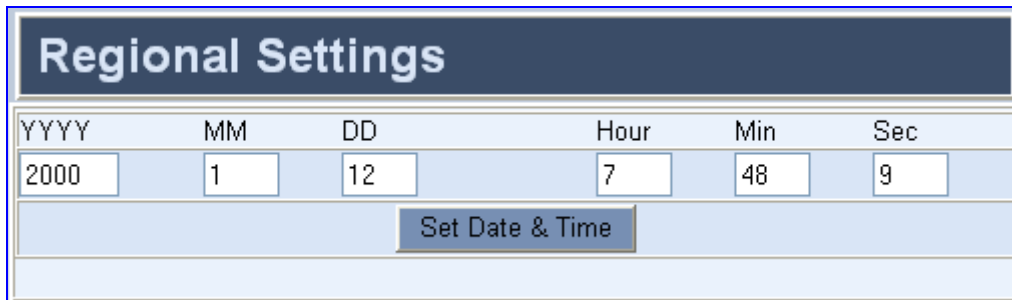
5.13.1 Regional Settings

The 'Regional Settings' screen allows you to define and view the gateway's internal date and time.

➤ **To configure the gateway's date and time, take these 3 steps:**

1. Open the 'Regional Settings' screen (**Advanced Configuration** menu > **Regional Settings**).

Figure 5-70: Regional Settings Screen



| YYYY | MM | DD | Hour | Min | Sec |
|------|----|----|------|-----|-----|
| 2000 | 1 | 12 | 7 | 48 | 9 |

Set Date & Time

2. Enter the time and date where the gateway is installed.
3. Click the **Set Date & Time** button; the date and time are automatically updated.



Notes:

- After performing a hardware reset, the date and time are returned to their defaults and should therefore be updated.
- For configuring the gateway to obtain the time from an SNTP server, refer to 'Simple Network Time Protocol Support' on page 430.

5.13.2 Locking and Unlocking the Gateway

The Lock and Unlock options allow you to lock the gateway so that it doesn't accept any new incoming calls. This is beneficial when, for example, you are uploading new software files to the gateway and you don't want any traffic to interfere with the process.

➤ **To lock the gateway, take these 4 steps:**

1. Open the 'Maintenance Actions' screen (**Maintenance** menu).

Figure 5-71: Maintenance Actions Screen

| Maintenance Actions | |
|---------------------|--------------------------------------|
| RESET | |
| Reset Board | <input type="button" value="Reset"/> |
| Burn To FLASH | <input type="button" value="Yes"/> |
| Graceful Option | <input type="button" value="No"/> |
| LOCK / UNLOCK | |
| Lock | <input type="button" value="LOCK"/> |
| Graceful Option | <input type="button" value="No"/> |
| Current Admin State | UNLOCKED |
| Save Configuration | |
| Save Configuration | <input type="button" value="BURN"/> |

2. Under the 'LOCK / UNLOCK' group, from the 'Graceful Option' drop-down list, select one of the following options:
 - 'Yes': The gateway is 'locked' only after the user-defined time in the 'Lock Timeout' field (refer to Step 3) expires or no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
 - 'No': The gateway is 'locked' regardless of traffic. Any existing traffic is terminated immediately.
3. In the 'Lock Timeout' field (relevant only if the 'Graceful Option' in the previous step is set to 'Yes'), enter the time (in seconds) after which the gateway locks. Note that if no traffic exists and the time has not yet expired, the gateway locks.
4. Click the **LOCK** button; If 'Graceful Option' is set to 'Yes', the lock is delayed and a screen displaying the number of remaining calls and time is displayed. Otherwise, the lock process begins immediately. The 'Current Admin State' field displays the current state: LOCKED or UNLOCKED.

➤ **To unlock the gateway, take these 2 steps:**

1. Access the 'Maintenance Actions' screen as described above in the previous procedure.
2. Click the **UNLOCK** button. Unlock starts immediately and the gateway is ready for new incoming calls.

5.13.3 Saving Configuration

The 'Maintenance Actions' screen enables you to save the current parameter configuration and the loaded auxiliary files to the gateway's *non-volatile* memory (i.e., flash) so they are available after a hardware reset (or power fail). Parameters that are only saved to the *volatile* memory (RAM) revert to their previous settings after a hardware reset.



Notes:

- Saving changes to the *non-volatile* memory may disrupt traffic on the gateway. To avoid this, disable all new traffic before saving by performing a graceful lock (refer to 'Locking and Unlocking the Gateway' on page 276).
- In the Embedded Web Server, parameters prefixed with an exclamation mark (!) are saved to the non-volatile memory only after a device reset.

➤ To save the changes to the non-volatile flash memory , take these 2 steps:

1. Open the 'Maintenance Actions' screen (**Maintenance** menu).

Figure 5-72: Maintenance Actions Screen

| Maintenance Actions | |
|----------------------------|--------------------------------------|
| RESET | |
| Reset Board | <input type="button" value="Reset"/> |
| Burn To FLASH | Yes <input type="button" value="v"/> |
| Graceful Option | No <input type="button" value="v"/> |
| LOCK / UNLOCK | |
| Lock | <input type="button" value="LOCK"/> |
| Graceful Option | No <input type="button" value="v"/> |
| Current Admin State | UNLOCKED |
| Save Configuration | |
| Save Configuration | <input type="button" value="BURN"/> |

2. Click the **BURN** button; a confirmation message appears when the save is completed successfully.

5.13.4 Resetting the Gateway

The 'Maintenance Actions' screen enables you to remotely reset the gateway. Before you reset the gateway, you can choose the following options:

- Save the gateway's current configuration to the flash memory (non-volatile).
- Perform a graceful shutdown. Reset starts only after a user-defined time expires or after no more active traffic exists (the earliest thereof).

➤ **To reset the gateway, take these 5 steps:**

1. Open the 'Maintenance Actions' screen (**Maintenance** menu).

Figure 5-73: Maintenance Actions Screen

| Maintenance Actions | |
|----------------------------|--------------------------------------|
| RESET | |
| Reset Board | <input type="button" value="Reset"/> |
| Burn To FLASH | Yes <input type="button" value="v"/> |
| Graceful Option | No <input type="button" value="v"/> |
| LOCK / UNLOCK | |
| Lock | <input type="button" value="LOCK"/> |
| Graceful Option | No <input type="button" value="v"/> |
| Current Admin State | UNLOCKED |
| Save Configuration | |
| Save Configuration | <input type="button" value="BURN"/> |

2. Under the 'RESET' group, from the 'Burn To FLASH' drop-down list, select one of the following options:
 - 'Yes': The gateway's current configuration is burned (i.e., saved) to the flash memory prior to reset (default).
 - 'No': Resets the device without burning (i.e., saving) the current configuration to flash (discards all unsaved modifications to the configuration).
3. Under the 'RESET' group, from the 'Graceful Option' drop-down list, select one of the following options:
 - 'Yes': Reset starts only after the user-defined time in the 'Shutdown Timeout' field (refer to Step 5) expires or after no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
 - 'No': Reset starts regardless of traffic and any existing traffic is terminated at once.

4. In the 'Shutdown Timeout' field (relevant only if the 'Graceful Option' in the previous step is set to 'Yes'), enter the time after which the gateway resets. Note that if no traffic exists and the time has not yet expired, the gateway resets.
5. Click the **RESET** button; If 'Graceful Option' is set to 'Yes', the reset is delayed and a screen displaying the number of remaining calls and time is displayed. When the device resets, a message is displayed informing of the waiting period.

5.13.5 Restoring and Backing up Configuration

The 'Configuration File' screen enables you to restore (load a new *ini* file to the gateway) or to back up (make a copy of the VoIP gateway *ini* file and store it in a directory on your computer) the current configuration the gateway is using.

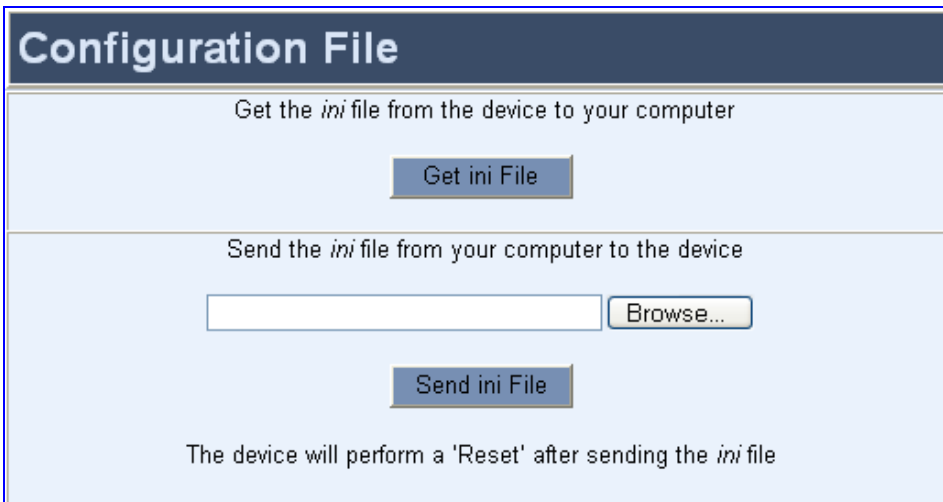
Back up your configuration if you want to protect your VoIP gateway programming. The backup *ini* file includes only those parameters that were modified and contain other than default values.

Restore your configuration if the VoIP gateway has been replaced or has lost its programming information, you can restore the VoIP gateway configuration from a previous backup or from a newly created *ini* file. To restore the VoIP gateway configuration from a previous backup you must have a backup of the VoIP gateway information stored on your computer.

➤ To restore or back up the *ini* file, take this step:

- Open the 'Configuration File' screen (**Advanced Configuration** menu > **Configuration File**).

Figure 5-74: Configuration File Screen



Configuration File

Get the *ini* file from the device to your computer

Get ini File

Send the *ini* file from your computer to the device

Browse...

Send ini File

The device will perform a 'Reset' after sending the *ini* file

➤ To back up the *ini* file on your PC, take these 4 steps:

1. Click the **Get ini File** button; the 'File Download' window opens.
2. Click the **Save** button; the 'Save As' window opens.
3. Navigate to the folder where you want to save the *ini* file on your PC.
4. Click the **Save** button; the VoIP gateway copies the *ini* file into the folder you selected.

➤ **To restore the *ini* file, take these 4 steps:**

1. Click the **Browse** button.
2. Navigate to the folder that contains the *ini* file you want to load.
3. Click the file and click the **Open** button; the name and path of the file appear in the field beside the Browse button.
4. Click the **Send *ini* File** button, and then at the prompt, click **OK**; the gateway is automatically reset (from the *cmp* version stored on the flash memory).

5.13.6 Factory Default Settings

5.13.6.1 Defining Default Values

The gateway is shipped with factory default configuration values stored on its non-volatile flash memory. However, you can re-define your own default values instead of using the factory defaults. This is performed using another *ini* file (in addition to the standard *ini* file) that includes [ClientDefaults] as the header. Below this header, simply define new default values for the required *ini* file parameters. The parameters are defined in the same format as in the standard *ini* file, and loaded to the gateway using TFTP (not via the Embedded Web Server).

➤ **To define default values for gateway parameters, take these 2 steps:**

1. Configure the ClientDefaults *ini* file with new default values for parameters, as needed.
2. Load the ClientDefaults *ini* file to the gateway using TFTP (refer to the *SIP Series Reference Manual*).

An example of the ClientsDefault *ini* file (changing default values for Syslog server parameters) is shown below:

```
[ClientDefaults]
EnableSyslog = 1
SyslogServerIP = 10.13.2.20
```

➤ **To remove user-defined defaults and restore factory default values, take this step:**

- Load an empty (i.e., without any parameters) ClientDefaults *ini* file to the gateway, using TFTP.

5.13.6.2 Restoring Default Settings

You can use the gateway's hardware Reset button to restore all the gateway's configuration settings to default (e.g., IP address and login username and password). These default settings include factory as well as user-defined (refer to 'Defining Default Values' on page 281) defaults, where user-defined defaults override corresponding factory defaults.

- **To restore the gateway to default settings, take this step:**
 - With a paper clip or any other similar pointed object, press and hold down the Reset button (located on the front panel) for about six seconds; the gateway is restored to its factory settings.

5.14 Using the Home Page

The **Home** icon, located above the main menu bar, opens the Home page. This page provides you with a graphical display of the gateway's front-panel and allows you to monitor various ports and interfaces, view alarms, assign names to ports, release analog channels, and replace modules.

5.14.1 Accessing the Home Page

- **To access the Home page, take this step:**


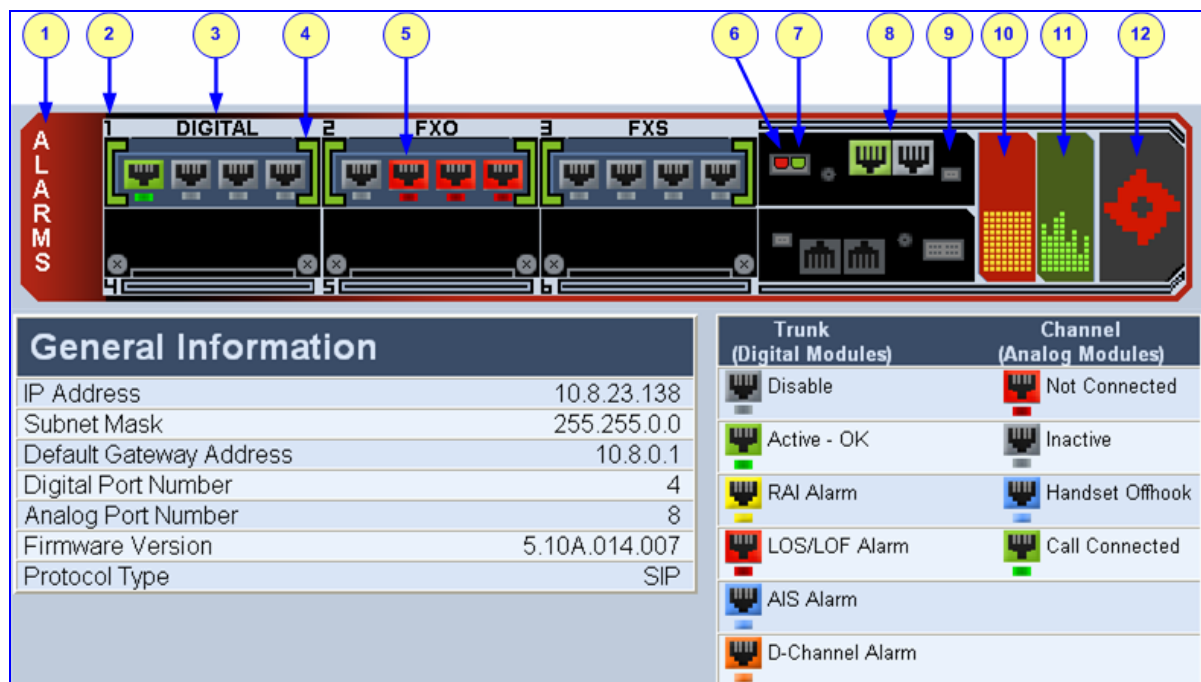
- Open the Home page by clicking the Home icon ; the Home page is displayed.

Figure 5-75: Graphical Display of the Hardware



The number of trunks and channels that appear in the screen depends on the system configuration. The Home page in the figure above depicts a system with one T1 span, an FXO module with three channels, and an FXS module.

The Home page also displays general information in the General Information pane. This information includes parameters such as the gateway's IP address, the number of digital and analog ports, and firmware version.

The table below describes the areas of the graphic display of the Mediant 1000 chassis.

Table 5-62: Description of the Areas of the Home Page

| Item# | Description |
|-------|---|
| 1 | ALARMS button for viewing the Active Alarms table. For a detailed description, refer to 'Viewing the Active Alarms Table' on page 288 . |
| 2 | Module slot number (1 to 6). |
| 3 | Module type (digital, FXO, or FXS). |
| 4 | Module status indicator. For a detailed description, refer to 'Monitoring the Modules' on page 287 . |
| 5 | Module's port (trunk or channel) status indicator. For a detailed description, refer to 'Monitoring the Mediant 1000 Trunks and Channels' on page 284 . |
| 6 | Dry Contact (normally open) status indicator. For a detailed description, refer to 'Monitoring Ethernet Ports, Dry Contacts, Power Supply Units, and Fan Tray Unit' on page 288 . |
| 7 | Dry Contact (normally closed) status indicator. For a detailed description, refer to 'Monitoring Ethernet Ports, Dry Contacts, Power Supply Units, and Fan Tray Unit' on page 288 . |
| 8 | Ethernet port status indicator (refer to 'Monitoring Ethernet Ports, Dry Contacts, Power Supply Units, and Fan Tray Unit' on page 288). If clicked, the 'Ethernet Port Information' screen opens (refer to 'Viewing Ethernet Port Settings' on page 289). |
| 9 | CPU module. |
| 10 | Power Supply Unit 1 status indicator. For a detailed description, refer to 'Monitoring Ethernet Ports, Dry Contacts, Power Supply Units, and Fan Tray Unit' on page 288 . |
| 11 | Power Supply Unit 2 status indicator. For a detailed description, refer to 'Monitoring Ethernet Ports, Dry Contacts, Power Supply Units, and Fan Tray Unit' on page 288 . |
| 12 | Fan tray unit status indicator. For a detailed description, refer to 'Monitoring Ethernet Ports, Dry Contacts, Power Supply Units, and Fan Tray Unit' on page 288 . |

5.14.2 Monitoring the Mediant 1000 Trunks and Channels







The Home page provides real-time monitoring of the trunks and channels.

➤ **To monitor the status of the Mediant 1000 trunks and channel ports, take this step:**

- Open the Home page by clicking the **Home** icon; the Home page is displayed.

The color of each trunk and FXO/FXS channel icon indicates the status of that trunk or channel. The table below describes the color-coding of the trunk and channel icons.

Table 5-63: Trunk and FXO/FXS Channel Status Color Indicators

| Trunk/Channel Status Icon | | Trunk (Digital Module) | | Channel (Analog Module) | |
|---|--------|------------------------|---|-------------------------|--|
| Indicator | Color | Label | Description | Label | Description |
|  | Grey | Disable | Trunk not configured (not in use) | Inactive | Channel is currently onhook |
|  | Green | Active - OK | Trunk synchronized | Call Connected | Active RTP stream |
|  | Yellow | RAI Alarm | Remote Alarm Indication (RAI), also known as the Yellow Alarm | -- | -- |
|  | Red | LOS/LOF Alarm | Loss due to LOS (Loss of Signal) or LOF (Loss of Frame) | Not Connected | No analog line is connected to this port (FXO only) |
|  | Blue | AIS Alarm | Alarm Indication Signal (AIS), also known as the Blue Alarm | Handset Offhook | Channel is offhook, but there is no active RTP session |
|  | Orange | D-Channel Alarm | D-channel alarm | -- | -- |

You can drill-down to view a detailed status of each channel pertaining to a trunk or FXO/FXS port.

➤ **To view a detailed status of a trunk, take these 4 steps:**

1. In the Home page, click the trunk of whose status you want to view; a shortcut menu appears.
2. From the shortcut menu, choose **Port Settings**; the 'Trunk & Channel Status' screen pertaining to the specific trunk appears:

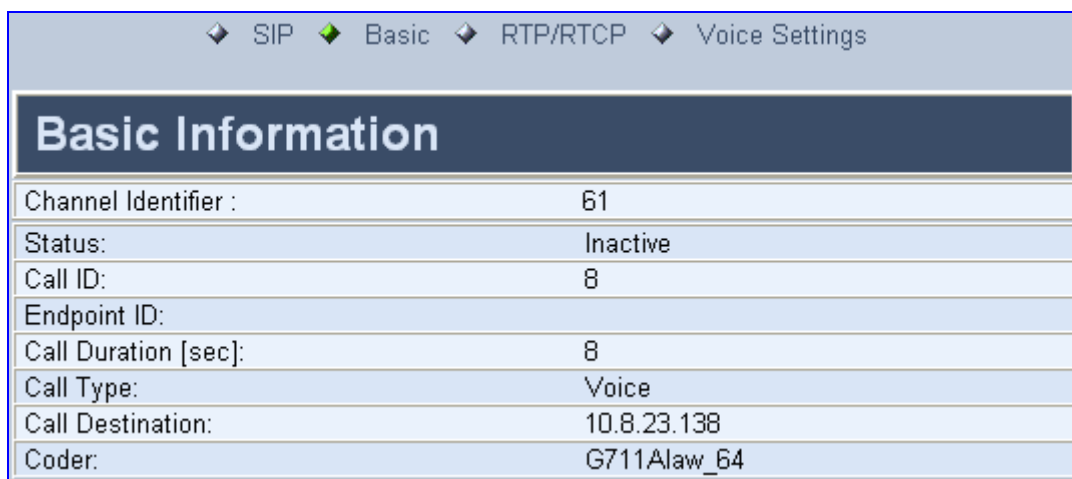
Figure 5-76: Trunk and Channel Status Screen



The trunk's channels are graphically displayed as icons. The colors of the icons depict the channels' statuses. For a description of the color coding for the channel status, refer to the table below.







3. To view the configuration settings of the trunk and / or to modify the trunk's settings, click the **Trunk** icon, and then from the shortcut menu, choose **Port Settings**; The 'Trunk Settings' screen appears. (For detailed information on configuring the trunk in this screen, refer to 'Trunk Settings' on page 206.)
4. To view information of a specific trunk's channel, click the required **Channel** icon; the 'Basic Information' screen appears:

Figure 5-77: Basic Information Screen



5. Click the buttons located above the 'Basic Information' screen to view additional parameters.





Table 5-64: Trunk's Channel Status Color Indicators

| Indicator | Color | Label | Description |
|---|-----------|-----------------------|--|
|  | Grey | Inactive | Configured, but currently no call |
|  | Green | Active | Call in progress (RTP traffic) |
|  | Pink | SS7 | Configured for SS7 (Currently not supported) |
|  | Dark blue | Non Voice | Not configured |
|  | Blue | ISDN Signaling | Configured as a D-channel |
|  | Yellow | CAS Blocked | -- |

➤ **To view a detailed status of an FXO or FXS channel, take these 3 steps:**

1. In the Home page, click the analog port of whose status you want to view; a shortcut menu appears.
2. From the shortcut menu, choose **Port Settings**; the 'Channel Status' screens.

Figure 5-78: Basic Information Screen

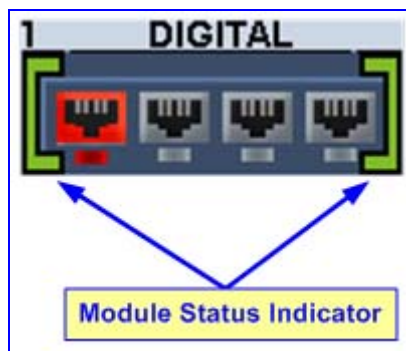
| | |
|---|-------------|
| <div>  SIP  Basic  RTP/RTCP  Voice Settings </div> | |
| Basic Information | |
| Channel Identifier : | 0 |
| Status: | Active |
| Call ID: | 8 |
| Endpoint ID: | |
| Call Duration [sec]: | 8 |
| Call Type: | Voice |
| Call Destination: | 10.8.23.138 |
| Coder: | G723Low |
| Line Current[mA]: | 0 |
| Line Voltage[V]: | 0 |
| Hook(0-Onhook, 1-Off hook): | 0 |
| Ring(0-Off, 1-On): | 0 |
| Line Connected(0-Disconnected, 1-Connected): | 1 |
| Polarity state(0-Normal, 1-Reversed, 2-N/A): | 0 |
| Line polarity(0-Positive, 1-Negative): | 0 |
| Message Waiting Indication(0-Off, 1-On): | 0 |

3. Click the buttons located above the 'Basic Information' screen to view additional parameters.

5.14.3 Monitoring the Modules




The Home page also provides color-coding for displaying the status of the modules (digital and analog). In the Home page, the color of the 'square brackets' enclosing the module depicts the status of the module.

Figure 5-79: Module Status Indicators



The color coding of the module status indicators are described in the table below:

Table 5-65: Description of the Module Status Indicators

| Indicator | Color | Description |
|---|-------|--|
|  | Green | Module has been inserted or is correctly configured. |
|  | Grey | Module was removed. 'Reserved' is displayed alongside the module's name. |
|  | Red | Module failure. 'Failure' is displayed instead of the module's name. |

5.14.4 Monitoring Ethernet Ports, Dry Contacts, Power Supply Units, and Fan Tray Unit

The Home page also displays the status of the Ethernet ports, Dry Contacts, power supply units, and fan tray unit. The table below describes the color-coding of the status indicators of these units:

Figure 5-80: Monitoring Ethernet, Power, Fan and Dry Contacts

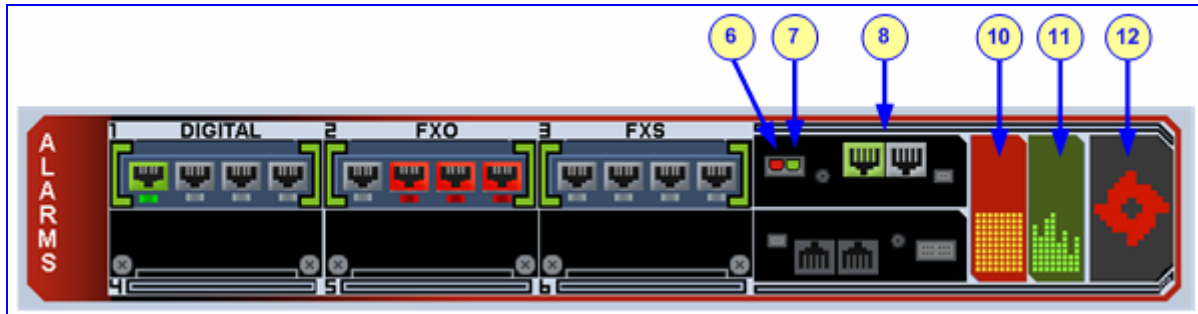


Table 5-66: Description of Ethernet Ports, Dry Contacts, Power Supply, and Fan Tray Indicators

| Item# | Unit | Color | Description |
|---------|--------------------|-------|--|
| 6 | Dry Contact | Green | Dry Contact is open (normal) |
| | | Red | Dry contact is closed |
| 7 | Dry Contact | Green | Dry Contact is closed (normal) |
| | | Red | Dry contact is open |
| 8 | Ethernet Port | Green | Ethernet link is working |
| | | Grey | Ethernet link not configured |
| 10 & 11 | Power Supply Units | Green | Power supply is operating |
| | | Red | Power supply failure or no power supply unit installed |
| 12 | Fan Tray Unit | Green | Fan tray operating |
| | | Red | Fan tray failure |

5.14.5 Viewing the Active Alarms Table

The Home page allows you to view a list of active alarms. These alarms are displayed in the 'Active Alarms' screen. For each alarm, the following is displayed:

■ **Severity:** severity level of the alarm:

- Critical: red
- Major: orange
- Minor: yellow
- No alarm: green

- **Source:** module or unit from which the alarm was raised
 - **Description:** brief explanation of the alarm
 - **Date:** date and time that the alarm was generated
- **To view a list of alarms, take these 2 steps:**
1. Open the Home page by clicking the **Home** icon; the Home page is displayed.
 2. On the graphical display of the Mediant 1000 front panel, click the area labelled '**ALARMS**' or any area that displays the tooltip 'Click To Get Active Alarms Table'; the 'Active Alarms' screen appears.

Figure 5-81: Active Alarms Screen

| Active Alarms | | | |
|---------------|-------------------------|---|-----------------------|
| Severity | Source | Description | Date |
| Critical | Chassis#0:FanTray#0 | Fan-Tray Alarm. Fan-Tray is missing | 10.1.2000 , 4:17:28.0 |
| Major | Chassis#0:PowerSupply#1 | Power Supply Alarm. Power Supply is missing | 10.1.2000 , 4:17:29.0 |

5.14.6 Viewing Ethernet Port Information

The 'Ethernet Port Information' screen provides read-only information on the Ethernet connection used by the Mediant 1000. Accessing this screen from the Home page provides an alternative to accessing it from the **Status & Diagnostics** menu (refer to 'Viewing Ethernet Port Information' on page 260).

- **To view Ethernet port settings, take this step:**


- In the Home page, click the Ethernet port status icon ; the 'Ethernet Port Information' screen opens.

Figure 5-82: Ethernet Port Information Screen

| Ethernet Port Information | |
|---------------------------|---------------|
| Active Port | 1 |
| Port 1 Duplex Mode | Half Duplex |
| Port 1 Speed | 100 Mbps |
| Port 2 Duplex Mode | Not Available |
| Port 2 Speed | Not Available |

For detailed information on the Ethernet parameters, refer to 'Viewing Ethernet Port Information' on page 260.

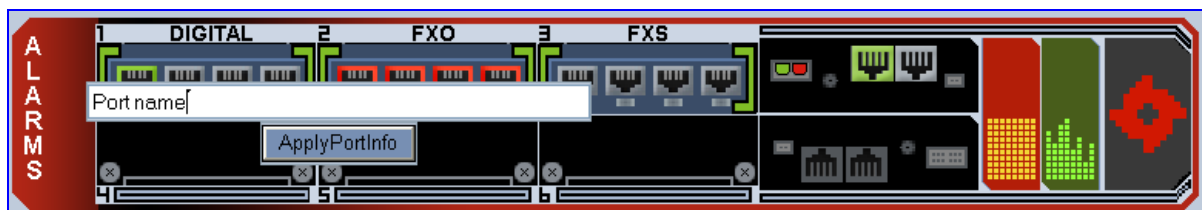
5.14.7 Assigning a Name or Brief Description to a Port

The Home page allows you to assign an arbitrary name or brief description to the gateway's ports. This description appears as a tooltip when you move your mouse over the specific port.

➤ **To add a port description, take these 4 steps:**

1. Open the Home page by clicking the **Home** icon.
2. Click the required port icon; a shortcut menu appears.
3. From the shortcut menu, choose **Update Port Info**; a text box appears.
4. Type a brief description for the port, and then click **Apply Port Info**.

Figure 5-83: Assigning a Port Name



5.14.8 Releasing an Analog Channel

The Home page allows you to inactivate (*release*) an FXO or FXS analog channel. This is sometimes useful in scenarios, for example, when the gateway (FXO) is connected to a PBX and the communication between the two can't be disconnected (e.g., when using reverse polarity).

➤ **To release a channel, take these 2 steps:**

1. Open the Home page by clicking the **Home** icon.
2. Click the required FXS or FXO port, and then from the shortcut menu, choose **Release Channel**; the channel is changed to inactive.

5.14.9 Replacing Modules

To replace modules (i.e., digital, FXO, and FXS), you must use the gateway's embedded Web server in combination with the physical removal and insertion of the modules. When you replace a module, you first need to 'remove' it in the Home page, then extract it physically from the chassis and physically insert a new module, and then 'insert' it in the Home page.

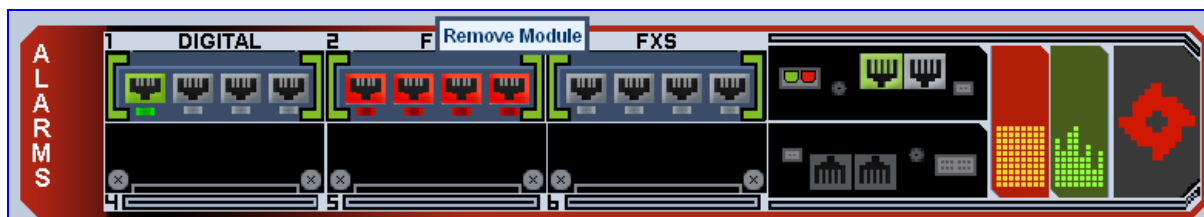
**Warnings:**

- Replacing of a damaged module can be performed only with the same module and in the exact module slot (e.g., a module with two digital spans in Slot 1 must be replaced with a module with two digital spans in Slot 1).
- When only one module is available, removal of the module causes the device to reset.
- Adding a module to a previously empty slot must only be performed when the power to the gateway is switched off (refer to 'Inserting Modules into Previously Empty Slots' on page 44)

➤ **To replace a module, take these 2 steps:**

1. Remove the module by performing the following:
 - a. On the Home page, click the top border line pertaining to the module that you want to replace; the **Remove Module** button appears.

Figure 5-84: Remove Module Button Appears after Clicking Module Name



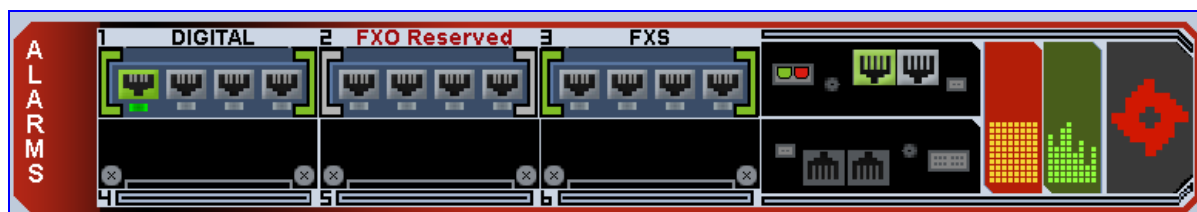
- b. Click the **Remove Module** button; a message box appears requesting you to confirm module removal.

Figure 5-85: Module Removal Confirmation Message Box

Table 5-67: []

- c. Click **OK** to confirm module removal; after a few seconds, the module is "removed" and the module status indicator is grayed. The name of the module is suffixed with the word 'Reserved'.

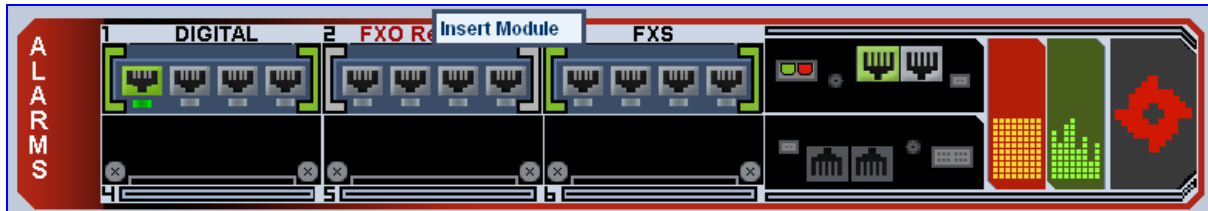
Figure 5-86: Removed Module



- d. You can now physically remove the module (refer to 'Replacing Modules' on page 43).

2. Insert the replaced module by performing the following:
 - a. Physically insert the replaced module (refer to 'Replacing Modules' on page 43).
 - b. On the Home page, click the top border line pertaining to the module that you want to replace; the **Insert Module** button appears.

Figure 5-87: Insert Module Button after Clicking Module's Name



- c. Click the **Insert Module** button; a message appears informing you that this may take a few seconds. When the message disappears, the module is inserted indicated by the disappearance of the 'Reserved' word from the module's name.

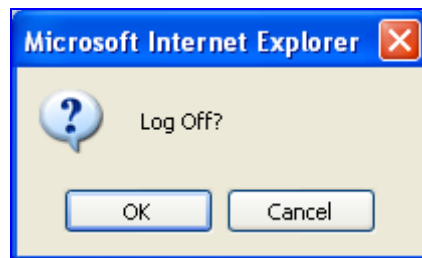
5.15 Logging Off the Embedded Web Server

The **Log Off** button enables you to log off the Embedded Web Server and to re-access it with a different account. For detailed information on the Web User Accounts, refer to 'User Accounts' on page 58.

➤ To log off the Embedded Web Server, take these 2 steps:

1. Click the **Log Off** button on the main menu bar; the 'Log Off' prompt screen is displayed.

Figure 5-88: Log Off Confirmation Box



2. Click **OK**; the Web session is logged off.

6 ini File Configuration

As an alternative to configuring the gateway using the Embedded Web Server (refer to 'Web-based Management' on page 57), you can configure the gateway by loading the *ini* file containing user-defined parameters.

The *ini* file is loaded via the BootP/TFTP utility (refer to the *SIP Series Reference Manual*) or via any standard TFTP server. It can also be loaded using the Embedded Web Server (refer to 'Restoring and Backing up Configuration' on page 280).

The *ini* file configuration parameters are saved in the gateway's non-volatile memory after the file is loaded to the gateway. When a parameter is absent from the *ini* file, the default value is assigned to that parameter (according to the *cmp* file loaded to the gateway) and stored in the non-volatile memory (thereby overriding the value previously defined for that parameter). Therefore, to restore the gateway's default configuration parameters, use the *ini* file without any valid parameters or with a semicolon (;) preceding all lines in the file.

Some of the gateway's parameters are configurable only through the *ini* file (and not via the Embedded Web Server). These parameters usually determine a low-level functionality and are seldom changed for a specific application.



Note: For a list of the *ini* file parameters, refer to 'The ini File Parameter Reference' on page 298. The *ini* file parameters that are configurable through the Embedded Web Server are described in 'Web-based Management' on page 57. Those *ini* parameters that can't be configured using the Embedded Web Server are described in this section.

6.1 Secured ini File

The *ini* file contains sensitive information that is required for the functioning of the gateway. It is loaded to, or retrieved from the device via TFTP or HTTP. These protocols are unsecured and vulnerable to potential hackers. Therefore, an encoded *ini* file significantly reduces these threats.

You can load an encoded *ini* file to the gateway. When you load an encoded *ini* file, the retrieved *ini* file is also encoded. Use the 'TrunkPack Downloadable Conversion Utility' to encode or decode the *ini* file before you load it to, or retrieve it from the device. Note that the encoded *ini* file's loading procedure is identical to the regular *ini* file's loading procedure. For information on encoding / decoding an *ini* file, refer to the *SIP Series Reference Manual*.

6.2 Modifying an ini File

➤ **To modify an *ini* file, take these 4 steps:**

1. Save the *ini* file from the gateway to your PC using the Embedded Web Server (refer to 'Restoring and Backing up Configuration' on page 280).
2. Open the *ini* file (using a text file editor such as Microsoft Notepad), and then modify the *ini* file parameters according to your requirements.

3. Save the new settings, and then close the file.
4. Load the modified *ini* file to the gateway (using either BootP/TFTP utility or the Embedded Web Server).

This method of modifying the *ini* file preserves the configuration that already exists in the device, including special default values that were preconfigured when the unit was manufactured.



Tip: Before loading the *ini* file to the gateway, verify that the file extension of the *ini* file saved on your PC is correct (i.e., *xxx.ini*). If the file extension name is not displayed, verify that the check box 'Hide extensions for known file types' (My Computer > Tools > Folder Options > View) is unchecked.

6.3 The ini File Content

The *ini* file contains the following gateway information:

- Networking parameters (refer to 'Networking Parameters' on page 299)
- System parameters (refer to 'System Parameters' on page 308)
- Web and Telnet parameters (refer to 'Web and Telnet Parameters' on page 315)
- Security parameters (refer to 'Security' on page 318)
- RADIUS parameters (refer to 'RADIUS Parameters' on page 320)
- SNMP parameters (refer to 'SNMP Parameters' on page 321)
- SIP Configuration parameters (refer to 'SIP Configuration Parameters' on page 323)
- Media Server parameters (refer to 'Media Server Parameters' on page 337)
- Voice Mail parameters (refer to 'Voice Mail Parameters' on page 338)
- PSTN parameters (refer to 'PSTN Parameters' on page 340)
- Analog Telephony parameters (refer to 'Analog Telephony Parameters' on page 350)
- Number Manipulation and Routing parameters (refer to 'Number Manipulation and Routing Parameters' on page 359)
- Channel Parameters (refer to 'Channel Parameters' on page 372)
- Configuration Files parameters (refer to 'Configuration Files Parameters' on page 378)

6.4 The ini File Structure

The *ini* file can contain any number of parameters. The *ini* file consists of individual parameters, which are conveniently grouped into subsections by their functionality, as well as table parameters, which include multiple *ini* file parameters. The *ini* file structure for the individual *ini* files and *ini* file parameter tables are described in 'Structure of Individual ini File Parameters' on page 295 and 'Configuring Parameter Tables Using the ini File' on page 295 respectively.

6.4.1 The ini File Structure Rules

The *ini* file must adhere to the following format rules:

- The *ini* file name must not include hyphens or spaces; use underscore instead.
- Lines beginning with a semi-colon (";") as the first character are ignored. These can be used for adding remarks in the *ini* file.
- A carriage return (i.e., Enter) must be the final character of each line.
- The number of spaces before and after the equals sign ("=") is not relevant.
- If there is a syntax error in the parameter name, the value is ignored.
- Syntax errors in the parameter value field can cause unexpected errors (parameters may be set to the incorrect values).
- Sub-section names are optional.
- String parameter values that denote file names (for example, for parameter CallProgressTonesFileName), must be placed between two inverted commas ('...').
- The parameter name is not case-sensitive.
- The parameter value is not case-sensitive, except for coder names.
- The *ini* file must end with at least one carriage return.

6.4.2 Structure of Individual ini File Parameters

The structure of the *ini* file containing individual *ini* file parameters is shown below:

```
[Subsection Name]
Parameter_Name = Parameter_Value
Parameter Name = Parameter Value
; REMARK
```

An example of an *ini* file containing individual *ini* file parameters is shown below:

```
[SYSTEM Params]
SyslogServerIP = 10.13.2.69
EnableSyslog = 1
; These are a few of the system-related parameters.
[WEB Params]
LogoWidth = '339'
WebLogoText = '10.8.210.21'
UseWeblogo = 1
; These are a few of the Web-related parameters.
```

6.4.3 Structure of ini File Parameter Tables

You can use the *ini* file to add / modify parameter tables. When using tables, read-only parameters are not loaded, as they cause an error when trying to reload the loaded file. Therefore, read-only parameters mustn't be included in tables in the *ini* file. Consequently, tables are loaded with all parameters having at least one of the following permissions: Write, Create or Maintenance Write.

Parameter tables (in an uploaded *ini* file) are grouped according to the applications they configure (e.g., NFS and IPSec). When loading an *ini* file to the gateway, the recommended policy is to include only tables that belong to applications that are to be configured (Dynamic tables of other applications are empty, but static tables are not).

A table is defined as a secret table if it contains at least one secret data field or if it depends on another secret table. A secret data field is a field that mustn't be revealed to the user. For example, in the IPSec application, IPSec tables are defined as secret tables as the IKE table contains a pre-shared key that must be concealed. Therefore, the SPD table that depends on the IKE table is defined as a secret table as well. Secret tables are never displayed in an uploaded *ini* file (e.g., when performing a 'Get *ini* File from Web' operation). Instead, there is a commented title that states that the secret table exists on the gateway, but is not to be revealed. Secret tables are always kept in the gateway's non-volatile memory and can be overwritten by new tables that are provided in a new *ini* file. If a secret table appears in an *ini* file, it replaces the current table regardless of its content. To delete a secret table from the gateway, provide an empty table of the same type (with no data lines) as part of a new *ini* file; the empty table replaces the previous table in the gateway.

The *ini* file includes a Format line that defines the columns of the table to be modified (this may vary from *ini* file to *ini* file for the same table). The Format line must only include columns that can be modified (parameters that are not specified as read-only). An exception is Index fields that are always mandatory.

Tables are composed of four elements:

- **Title of the table:** The name of the table in square brackets (e.g., [MY_TABLE_NAME]).
- **Format line:** Specifies the columns (parameters) of the table (by their string names) that are to be configured.
 - The first word of the Format line must be 'FORMAT', followed by the Index field name, and then an equal sign '='. After the equal sign the names of the columns (parameters) are listed.
 - Items must be separated by a comma ','.
 - The Format line must end with a semicolon ';'.
- **Data line(s):** Contain the actual values of the parameters. The values are interpreted according to the Format line. The first word of the Data line must be the table's string name followed by the Index fields.
 - Items must be separated by a comma ','.
 - A Data line must end with a semicolon ';'.
- **End-of-Table-Mark:** Indicates the end of the table. The same string used for the table's title, preceded by a backslash '\' (e.g., [\\MY_TABLE_NAME]).

The following displays an example of the structure of an *ini* file parameter table.

```
[Table Title]
; This is the title of the table.
FORMAT Item Index = Item Name1, Item Name2, Item Name3;
; This is the Format line.
Item 0 = value1, value2, value3;
Item 1 = value1, $$, value3;
; These are the Data lines.
[\\Table Title]
; This is the end-of-the-table-mark.
```

Refer to the following notes:

- Indices (in both the Format and the Data lines) must appear in the same order determined by the specific table's documentation. The Index field must never be omitted.
- The Format line can include a sub-set of the configurable fields in a table. In this case, all other fields are assigned with the pre-defined default values for each configured line.
- The order of the fields in the Format line isn't significant (as opposed to the Index-fields). The fields in the Data lines are interpreted according to the order specified in the Format line.
- The sign '\$\$' in a Data line indicates that the user wants to assign the pre-defined default value to it.
- The order of the Data lines is insignificant.
- Data lines must match the Format line, i.e., it must contain exactly the same number of Indices and Data fields and must be in exactly the same order.
- A line in a table is identified by its table-name and Index fields. Each such line may appear only once in the *ini* file.
- Table dependencies:
Certain tables may depend on other tables. For example, one table may include a field that specifies an entry in another table. This method is used to specify additional attributes of an entity, or to specify that a given entity is part of a larger entity. The tables must appear in the order of their dependency (i.e., if Table X is referred to by Table Y, Table X must appear in the *ini* file before Table Y). appear in the order of their dependency (i.e., if Table X is referred to by Table Y, Table X must appear in the *ini* file before Table Y).

The table below displays an example of an *ini* file parameter table:

```
[ PREFIX ]
FORMAT PREFIX Index = PREFIX DestinationPrefix,
PREFIX DestAddress, PREFIX SourcePrefix, PREFIX ProfileId,
PREFIX MeteringCode, PREFIX DestPort;
PREFIX 0 = 10, 10.13.83.5, *, 0, 255, 0;
PREFIX 1 = 20, 10.13.83.7, *, 0, 255, 0;
PREFIX 2 = 30, 10.13.83.6, *, 0, 255, 0;
PREFIX 3 = 20, 10.13.83.2, *, 0, 255, 0;
[ \PREFIX ]
```

6.4.4 The ini File Example

Below is an example of an *ini* file for the VoIP gateway.

```
PCMLawSelect = 1
ProtocolType = 1
TerminationSide = 0
FramingMethod = 0
LineCode = 2
TDMBusClockSource = 4
ClockMaster = 0
;Channel Params
DJBufMinDelay = 75
RTPRedundancyDepth = 1
IsProxyUsed = 1
ProxyIP = 192.168.122.179
[CoderName]
FORMAT CoderName Index = CoderName Type, CoderName PacketInterval,
CoderName rate, CoderName PayloadType, CoderName Sce;
CoderName 1= g7231,90
[\\CoderName]

;List of serial B-channel numbers
[TrunkGroup]
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum,
TrunkGroup_FirstTrunkId,TrunkGroup_LastTrunkId, TrunkGroup_FirstBChannel,
TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId,
TrunkGroup_Module;
TrunkGroup 1 = 0,0,0,1,24,1000;
TrunkGroup 2 = 0,1,1,1,24,2000;
TrunkGroup 3 = 0,2,2,1,24,3000;
TrunkGroup 4 = 0,3,3,1,24,4000;
[\\TrunkGroup]
EnableSyslog = 1
SyslogServerIP = 10.2.2.1
CallProgressTonesFilename = 'CPUSA.dat'
CASFileName = 'E_M_WinkTable.dat'
SaveConfiguration = 1
```

6.5 The ini File Parameter Reference

The subsections below list all the *ini* file parameters. References to their descriptions in the Embedded Web Server are provided, except for those *ini* file parameters that can only be configured using the *ini* file (and not the Embedded Web Server).

6.5.1 Networking Parameters

Table 6-1: Networking Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| EthernetPhyConfiguration | <p>Defines the Ethernet connection mode type.</p> <ul style="list-style-type: none"> ▪ [0] = 10 Base-T half-duplex ▪ [1] = 10 Base-T full-duplex ▪ [2] = 100 Base-TX half-duplex ▪ [3] = 100 Base-TX full-duplex ▪ [4] = Auto-negotiate (default) <p>For detailed information on Ethernet interface configuration, refer to 'Ethernet Interface Configuration' on page 423.</p> |
| MIIRedundancyEnable | <p>Enables the Ethernet Interface Redundancy feature. When enabled, the gateway performs a switchover to the secondary (redundant) Ethernet port upon sensing a link failure in the primary Ethernet port. When disabled, the gateway operates with a single port (i.e. no redundancy support).</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>For detailed information on Ethernet interface redundancy, refer to 'Ethernet Interface Redundancy' on page 423. Note: For this parameter to take effect, a gateway reset is required.</p> |
| DHCPEnable | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178 . |
| EnableLANWatchDog | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| DNSPriServerIP | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178 . |
| DNSSecServerIP | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178 . |

Table 6-1: Networking Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| DNS2IP | <p>The Internal DNS table is used to resolve host names to IP addresses. Two different IP addresses (in dotted format notation) can be assigned to a hostname.</p> <p>The format of this <i>ini</i> file parameter table is as follows:</p> <pre>[Dns2Ip] FORMAT Dns2Ip_Index = Dns2Ip_DomainName, Dns2Ip_FirstIpAddress, Dns2Ip_SecondIpAddress; [Dns2Ip]</pre> <p>Where,</p> <ul style="list-style-type: none"> DomainName = host name FirstIpAddress = first IP address SecondIpAddress = second IP address <p>For example:</p> <pre>[Dns2Ip] Dns2Ip 0 = DnsName, 1.1.1.1, 2.2.2.2; [Dns2Ip]</pre> <p>Notes:</p> <ul style="list-style-type: none"> If the internal DNS table is used, the gateway first attempts to resolve a domain name using this table. If the domain name isn't found, the gateway performs a DNS resolution using an external DNS server. This parameter can appear up to 10 times. For an explanation on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. |

Table 6-1: Networking Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| SRV2IP | <p>Defines the Internal SRV table used for resolving host names to DNS A-Records. Three different A-Records can be assigned to a hostname. Each A-Record contains the host name, priority, weight, and port. Format for this <i>ini</i> file parameter table:</p> <pre>[SRV2IP] FORMAT SRV2IP_Index = SRV2IP_InternalDomain, SRV2IP_TransportType, SRV2IP_Dns1, SRV2IP_Priority1, SRV2IP_Weight1, SRV2IP_Port1, SRV2IP_Dns2, SRV2IP_Priority2, SRV2IP_Weight2, SRV2IP_Port2, SRV2IP_Dns3, SRV2IP_Priority3, SRV2IP_Weight3, SRV2IP_Port3; [SRV2IP]</pre> <p>Where,</p> <ul style="list-style-type: none"> InternalDomain = Internal domain name TransportType = Transport type Dns1, Dns2, Dns3 = DNS name 1, 2, and 3 Priority1, Priority2, Priority3 = Priority 1, 2, and 3 Weight1, Weight2, Weight3 = Weight 1, 2, and 3 Port1, Port2, Port3 = Port 1, 2, and 3 <p>For example:</p> <pre>[SRV2IP] SRV2IP 0 = SrvDomain,0,Dnsname1,1,1,500,Dnsname2,2,2,501,\$\$,0,0,0; [SRV2IP]</pre> <p>Notes:</p> <ul style="list-style-type: none"> If the internal SRV table is used, the gateway first attempts to resolve a domain name using this table. If the domain name isn't located, the gateway performs an SRV resolution using an external DNS server. This parameter can appear up to 10 times. To configure the Internal SRV table using the Embedded Web Server, refer to 'Internal SRV Table' on page 141. For an explanation on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. |
| EnableSTUN | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |
| STUNServerPrimaryIP | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |
| STUNServerSecondaryIP | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |
| STUNServerDomainName | <p>Defines the domain name for the Simple Traversal of User Datagram Protocol (STUN) server's address (used for retrieving all STUN servers with an SRV query). The STUN client can perform the required SRV query to resolve this domain name to an IP address and port, sort the server list, and use the servers according to the sorted list.</p> <p>Note: Use either the STUNServerPrimaryIP or the STUNServerDomainName parameter, with priority to the first one.</p> |

Table 6-1: Networking Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| NATBindingDefaultTimeout | Defines the default NAT binding lifetime in seconds. STUN is used to refresh the binding information after this time expires. The valid range is 0 to 2,592,000. The default value is 30. |
| DisableNAT | Enables / disables the Network Address Translation (NAT) mechanism. <ul style="list-style-type: none"> [0] = Enabled. [1] = Disabled (default). Note: The compare operation that is performed on the IP address is enabled by default and is controlled by the parameter EnableIPAddrTranslation. The compare operation that is performed on the UDP port is disabled by default and is controlled by the parameter EnableUDPPortTranslation. |
| EnableIPAddrTranslation | <ul style="list-style-type: none"> [0] = Disable IP address translation. [1] = Enable IP address translation for RTP, RTCP and T.38 packets (default). [2] = Enable IP address translation for ThroughPacket™. [3] = Enable IP address translation for all protocols (RTP, RTCP, T38 and ThroughPacket™). When enabled, the gateway compares the source IP address of the first incoming packet, to the remote IP address stated in the opening of the channel. If the two IP addresses don't match, the NAT mechanism is activated. Consequently, the remote IP address of the outgoing stream is replaced by the source IP address of the first incoming packet. Note: The NAT mechanism must be enabled for this parameter to take effect (DisableNAT = 0). |
| EnableUDPPortTranslation | <ul style="list-style-type: none"> [0] = Disable UDP port translation (default). [1] = Enable UDP port translation. When enabled, the gateway compares the source UDP port of the first incoming packet, to the remote UDP port stated in the opening of the channel. If the two UDP ports don't match, the NAT mechanism is activated. Consequently, the remote UDP port of the outgoing stream is replaced by the source UDP port of the first incoming packet. Note: The NAT mechanism and the IP address translation must be enabled for this parameter to take effect (DisableNAT = 0, EnableIPAddrTranslation = 1). |
| NoOpEnable | Enables or disables the transmission of RTP or T.38 No-Op packets. <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods. |
| NoOpInterval | Defines the time interval in which RTP or T.38 No-Op packets are sent in the case of silence (no RTP / T.38 traffic) when No-Op packet transmission is enabled. The valid range is 20 to 65,000 msec. The default is 10,000. Note: To enable No-Op packet transmission, use the NoOpEnable parameter. |

Table 6-1: Networking Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| RTPNoOpInterval | This parameter is obsolete; use the parameter NoOpInterval. |
| RTPNoOpPayloadType | Determines the payload type of No-Op packets. the valid range is 96 to 127 (for the range for Dynamic RTP Payload Type for all types of non hard-coded RTP Payload types, refer to RFC 3551). The default value is 120. Note: When defining this parameter, ensure that it doesn't cause collision with other payload types. |
| EnableDetectRemoteMACChange | Changes the RTP packets according to the MAC address of received RTP packets and according to Gratuitous Address Resolution Protocol (GARP) messages. <ul style="list-style-type: none"> ▪ [0] = nothing is changed. ▪ [1] = If the gateway receives RTP packets with a different source MAC address (than the MAC address of the transmitted RTP packets), then it sends RTP packets to this MAC address and removes this IP entry from the gateway's ARP cache table. ▪ [2] = The gateway uses the received GARP packets to change the MAC address of the transmitted RTP packets. ▪ [3] = both 1 and 2 options above are used (default). |
| StaticNatIP | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| SyslogServerIP | For a description of this parameter, refer to 'Configuring the Management Settings' on page 243. |
| SyslogServerPort | For a description of this parameter, refer to 'Configuring the Management Settings' on page 243. |
| EnableSyslog | For a description of this parameter, refer to 'Configuring the Management Settings' on page 243. |
| BaseUDPport | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| RemoteBaseUDPport | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| L1L1ComplexTxUDPport | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| L1L1ComplexRxUDPport | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| NTPServerIP | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |
| NTPServerUTCOffset | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |
| NTPUpdateInterval | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |

Table 6-1: Networking Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|---|
| IP Routing Table parameters: The IP routing <i>ini</i> file parameters are array parameters. Each parameter configures a specific column in the IP routing table. The first entry in each parameter refers to the first row in the IP routing table, the second entry to the second row and so forth. In the following example, two rows are configured when the gateway is in network 10.31.x.x: RoutingTableDestinationsColumn = 130.33.4.6, 83.4.87.6 RoutingTableDestinationMasksColumn = 255.255.255.255, 255.255.255.0 RoutingTableGatewaysColumn = 10.31.0.1, 10.31.0.112 RoutingTableInterfacesColumn = 0, 1 RoutingTableHopsCountColumn = 20, 20 | |
| RoutingTableDestinationsColumn | For a description of this parameter, refer to 'Configuring the IP Routing Table' on page 186. |
| RoutingTableDestinationMasksColumn | For a description of this parameter, refer to 'Configuring the IP Routing Table' on page 186. |
| RoutingTableGatewaysColumn | For a description of this parameter, refer to 'Configuring the IP Routing Table' on page 186. |
| RoutingTableHopsCountColumn | For a description of this parameter, refer to 'Configuring the IP Routing Table' on page 186. |
| RoutingTableInterfacesColumn | For a description of this parameter, refer to 'Configuring the IP Routing Table' on page 186. |
| VLAN Parameters | |
| VLANMode | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |
| VLANNativeVLANID | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |
| VLANOamVLANID | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |
| VLANControlVLANID | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |
| VLANMediaVLANID | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |
| VLANNetworkServiceClassPriority | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |
| VLANPremiumServiceClassMediaPriority | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |
| VLANPremiumServiceClassControlPriority | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |
| VlanGoldServiceClassPriority | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |
| VLANBronzeServiceClassPriority | For a description of this parameter, refer to 'Configuring the VLAN Settings' on page 188. |

Table 6-1: Networking Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| EnableDNSasOAM | This parameter applies to both Multiple IPs and VLAN mechanisms. Multiple IPs: Determines the network type for DNS services. VLAN: Determines the traffic type for DNS services. <ul style="list-style-type: none"> ▪ [1] = OAM (default) ▪ [0] = Control. |
| EnableNTPasOAM | This parameter applies to both Multiple IPs and VLAN mechanisms. Multiple IPs: Determines the network type for NTP services. VLAN: Determines the traffic type for NTP services. <ul style="list-style-type: none"> ▪ [1] = OAM (default) ▪ [0] = Control. |
| VLANSendNonTaggedOnNative | Specify whether to send non-tagged packets on the native VLAN. <ul style="list-style-type: none"> ▪ [0] = Sends priority tag packets (default). ▪ [1] = Sends regular packets (with no VLAN tag). |
| Multiple IPs Parameters | |
| EnableMultipleIPs | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| LocalMediaIPAddress | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| LocalMediaSubnetMask | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| LocalMediaDefaultGW | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| LocalControlIPAddress | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| LocalControlSubnetMask | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| LocalControlDefaultGW | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| LocalOAMIPAddress | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| LocalOAMSubnetMask | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| LocalOAMDefaultGW | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| PPPoE Parameters | |
| EnablePPPoE | Enables the PPPoE (Point-to-Point Protocol over Ethernet) feature. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable |
| PPPoEUserName | User Name for PAP or Host Name for CHAP authentication. The valid range is a string of up to 47 characters. The default value is 0. |

Table 6-1: Networking Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|--|
| PPPoEPassword | Password for PAP or Secret for CHAP authentication. The valid range is a string of up to 47 characters. The default value is 0. |
| PPPoEServerName | Server Name for CHAP authentication. The valid range is a string of up to 47 characters. The default value is 0. |
| PPPoEStaticIPAddress | IP address to use in a static configuration setup. If set, used during PPP negotiation to request this specific IP address from the PPP server. If approved by the server, this IP address is used during the session. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 0.0.0.0. |
| PPPoERecovertIPAddress | IP address to use when booting from the flash to non-PPPoE (Point-to-Point Protocol over Ethernet) environments. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 10.4.10.4. |
| PPPoERecovertSubnetMask | Subnet Mask to use when booting from the flash to non-PPPoE (Point-to-Point Protocol over Ethernet) environments. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 255.255.0.0. |
| PPPoERecovertDefaultGatewayAddress | Default Gateway address to use when booting from the flash to non-PPPoE (Point-to-Point Protocol over Ethernet) environments. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 10.4.10.1. |
| PPPoELCPEchoEnable | Enables or disables the Point-to-Point Protocol over Ethernet (PPPoE) disconnection auto-detection feature. <ul style="list-style-type: none"> [0] = Disable [1] = Enable (default) <p>By default, the PPPoE Client (i.e., embedded in the gateway) sends LCP Echo packets to the server to check that the PPPoE connection is open. Some Access Concentrators (PPPoE servers) don't reply to these LCP Echo requests, resulting in a disconnection. By disabling the LCP disconnection auto-detection feature, the PPPoE Client doesn't send LCP Echo packets to the server (and does not detect PPPoE disconnections).</p> |
| Differential Services. For detailed information on IP QoS via Differentiated Services, refer to 'IP QoS via Differentiated Services (DiffServ)' on page 430 . | |
| NetworkServiceClassDiffServ | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178 . |
| PremiumServiceClassMediaDiffServ | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178 . |
| PremiumServiceClassControlDiffServ | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178 . |
| GoldServiceClassDiffServ | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178 . |

Table 6-1: Networking Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| BronzeServiceClassDiffServ | For a description of this parameter, refer to 'Configuring the IP Settings' on page 178. |
| NFS Table Parameters (NFSServers) For an NFS <i>ini</i> file example, refer to 'Configuring the NFS Settings' on page 184. | |
| NFSServers_Index | For a description of this parameter, refer to 'Configuring the NFS Settings' on page 184. |
| NFSServers_HostOrIP | For a description of this parameter, refer to 'Configuring the NFS Settings' on page 184. |
| NFSServers_RootPath | For a description of this parameter, refer to 'Configuring the NFS Settings' on page 184. |
| The combination of Host / IP and Root Path must be unique for each row in the table. For example, there must be only one row in the table with a Host / IP of 192.168.1.1 and Root Path of /audio. | |
| NFSServers_NfsVersion | For a description of this parameter, refer to 'Configuring the NFS Settings' on page 184. |
| NFSServers_AuthType] | For a description of this parameter, refer to 'Configuring the NFS Settings' on page 184. |
| NFSServers_UID | For a description of this parameter, refer to 'Configuring the NFS Settings' on page 184. |
| NFSServers_GID | For a description of this parameter, refer to 'Configuring the NFS Settings' on page 184. |
| NFSServers_VLANType] | For a description of this parameter, refer to 'Configuring the NFS Settings' on page 184. |

6.5.2 System Parameters

Table 6-2: System Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| GroundKeyDetection | <p>Enables analog ground key detection (FXS and FXO modules implement ground start signaling) per gateway. When disabled, the gateway uses loop start signaling.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable (enables ground start) <p>Notes:</p> <ul style="list-style-type: none"> ▪ For ground start signaling, ensure that the FXO G module is installed (and not the regular FXO module) in the Mediant 1000. ▪ For ground start FXO, the following parameters should be configured: EnableCurrentDisconnect = 1; FXOBetweenRingTime = 300. |
| EnableDiagnostics | <p>Checks the correct functionality of the different hardware components on the gateway. On completion of the check, if the test fails, the gateway sends information on the test results of each hardware component to the Syslog server.</p> <ul style="list-style-type: none"> ▪ [0] = Rapid and Enhanced self-test mode (default). ▪ [1] = Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY and Flash). ▪ [2] = A quicker version of the Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY, but partial test of Flash). <p>For detailed information, refer to the <i>SIP Series Reference Manual</i>.</p> |
| WatchDogStatus | <ul style="list-style-type: none"> ▪ [0] = Disable gateway's watch dog. ▪ [1] = Enable gateway's watch dog (default). |
| LifeLineType | <p>Defines the Lifeline phone type. The Lifeline phone is available on port 1 of each analog module.</p> <p>The Lifeline is activated upon one of the following options:</p> <ul style="list-style-type: none"> ▪ [0] = Power down (default). ▪ [1] = Power down or when link is down (physical disconnect). ▪ [2] = Power down or when link is down or on network failure (logical link disconnect). <p>Notes:</p> <ul style="list-style-type: none"> ▪ To enable Lifeline switching on network failure, LAN watch dog must be activated (EnableLANWatchDog = 1). ▪ This parameter is only applicable to FXS interface. |
| GWAppDelayTime | <p>For a description of this parameter, refer to 'General Parameters' on page 103.</p> |

Table 6-2: System Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| ActivityListToLog | <p>The Activity Log mechanism enables the gateway to send log messages (to a Syslog server) that report certain types of Web actions according to a pre-defined filter.</p> <p>The following filters are available:</p> <ul style="list-style-type: none"> ▪ [PVC] (Parameters Value Change) - Changes made on-the-fly to parameters. ▪ [AFL] (Auxiliary Files Loading) - Loading of auxiliary files (e.g., via Certificate screen). ▪ [DR] (Device Reset) - Device reset via the Maintenance screen. ▪ [FB] (Flash Memory Burning) - Burning of files / parameters to flash (e.g., Maintenance screen). ▪ [SWU] (Device Software Update) - cmp loading via the Software Upgrade Wizard. ▪ [ARD] (Access to Restricted Domains) - Access to Restricted Domains. The following screens are restricted: (1) ini parameters (AdminPage) (2) General Security Settings (3) Configuration File (4) IPSec/IKE tables (5) Software Upgrade Key (6) Internal Firewall (7) Web Access List. (8) Web User Accounts ▪ [NAA] (Non Authorized Access) - Attempt to access the Embedded Web Server with a false / empty username or password. ▪ [SPC] (Sensitive Parameters Value Change) - Changes made to sensitive parameters: (1) IP Address (2) Subnet Mask (3) Default Gateway IP Address (4) ActivityListToLog <p>For example: ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc'</p> |
| ECHybridLoss | <p>Sets the four wire to two wire worst case Hybrid loss, the ratio between the signal level sent to the hybrid and the echo level returning from the hybrid.</p> <ul style="list-style-type: none"> ▪ [0] = 6 dB (default) ▪ [1] = N/A ▪ [2] = 0 dB ▪ [3] = 3 dB |
| GwDebugLevel | For a description of this parameter, refer to 'General Parameters' on page 103. |
| CDRReportLevel | For a description of this parameter, refer to 'General Parameters' on page 103. |

Table 6-2: System Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| CDRSyslogServerIP | For a description of this parameter, refer to 'General Parameters' on page 103. |
| HeartBeatDestIP | Destination IP address (in dotted format notation) to which the gateway sends proprietary UDP 'ping' packets. The default IP address is 0.0.0.0. |
| HeartBeatDestPort | Destination UDP port to which the heartbeat packets are sent. The range is 0 to 64000. The default is 0. |
| HeartBeatIntervalmsec | Delay (in msec) between consecutive heartbeat packets. <ul style="list-style-type: none"> [10] = 100000. [-1] = disabled (default). |
| EnableRAI | <ul style="list-style-type: none"> [0] = Disable RAI (Resource Available Indication) service (default). [1] = Enable RAI service. <p>If RAI is enabled, an SNMP 'acBoardCallResourcesAlarm' Alarm Trap is sent if gateway's busy endpoints exceed a predefined (configurable) threshold.</p> |
| RAIHighThreshold | High Threshold (in percentage) that defines the gateway's busy endpoints. The range is 0 to 100. The default value is 90%. When the percentage of the gateway's busy endpoints exceeds the value configured in High Threshold, the gateway sends an SNMP 'acBoardCallResourcesAlarm' Alarm Trap with a 'major' Alarm Status. Note: The percentage of busy endpoints is calculated by dividing the number of busy endpoints by the total number of "enabled" endpoints (trunks are physically connected and synchronized with no alarms and endpoints are defined in the Trunk Group table). |
| RAILowThreshold | Low Threshold (in percentage) that defines the gateway's busy endpoints. The range is 0 to 100. The default value is 90%. When the percentage of the gateway's busy endpoints falls below the value defined in Low Threshold, the gateway sends an SNMP 'acBoardCallResourcesAlarm' Alarm Trap with a 'cleared' Alarm Status. |
| RAILoopTime | Time interval (in seconds) that the gateway checks for resource availability. The default is 10 seconds. |
| Disconnect Supervision Parameters | |
| DisconnectOnBrokenConnection | For a description of this parameter, refer to 'General Parameters' on page 103. |
| BrokenConnectionEventTimeout | For a description of this parameter, refer to 'General Parameters' on page 103. |
| EnableSilenceDisconnect | For a description of this parameter, refer to 'General Parameters' on page 103. |
| FarEndDisconnectSilencePeriod | For a description of this parameter, refer to 'General Parameters' on page 103. |

Table 6-2: System Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| FarEndDisconnectSilenceMethod | For a description of this parameter, refer to 'General Parameters' on page 103. |
| FarEndDisconnectSilenceThreshold | Threshold of the packet count (in percents), below which is considered silence by the gateway. The valid range is 1 to 100. The default is 8%. Note: Applicable only if silence is detected according to packet count (FarEndDisconnectSilenceMethod = 1). |
| Automatic Update Parameters | |
| CmpFileURL | Specifies the name of the <i>cmp</i> file and the location of the server (IP address or FQDN) from which the gateway loads a new <i>cmp</i> file and updates itself. The <i>cmp</i> file can be loaded using: HTTP, HTTPS, FTP, FTPS or NFS. For example: http://192.168.0.1/filename Notes: <ul style="list-style-type: none"> When this parameter is set in the <i>ini</i> file, the gateway always loads the <i>cmp</i> file after it is reset. The <i>cmp</i> file is validated before it's burned to flash. The checksum of the <i>cmp</i> file is also compared to the previously-burnt checksum to avoid unnecessary resets. The maximum length of the URL address is 99 characters. |
| IniFileURL | Specifies the name of the <i>ini</i> file and the location of the server (IP address or FQDN) from which the gateway loads the <i>ini</i> file. The <i>ini</i> file can be loaded using: HTTP, HTTPS, FTP, FTPS or NFS. For example: http://192.168.0.1/filename http://192.8.77.13/config<MAC> https://<username>:<password>@<IP address>/<file name> Notes: <ul style="list-style-type: none"> When using HTTP or HTTPS, the date and time of the <i>ini</i> file are validated. Only more recently-dated <i>ini</i> files are loaded. The optional string '<MAC>' is replaced with the gateway's MAC address. Therefore, the gateway requests an <i>ini</i> file name that contains its MAC address. This option enables loading different configurations for specific gateways. The maximum length of the URL address is 99 characters. |
| PrtFileURL | Specifies the name of the Prerecorded Tones file and the location of the server (IP address or FQDN) from which it is loaded. For example: http://server_name/file, https://server_name/file. Note: The maximum length of the URL address is 99 characters. |
| CptFileURL | Specifies the name of the CPT file and the location of the server (IP address or FQDN) from which it is loaded. For example: http://server_name/file, https://server_name/file. Note: The maximum length of the URL address is 99 characters. |

Table 6-2: System Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|--|
| FXSCoeffFileURL | Specifies the name of the FXS coefficients file and the location of the server (IP address or FQDN) from where it is loaded. http://server_name/file, https://server_name/file. Note: The maximum length of the URL address is 99 characters. |
| FXOCoeffFileURL | Specifies the name of the FXO coefficients file and the location of the server (IP address or FQDN) from which it is loaded. For example: http://server_name/file, https://server_name/file. Note: The maximum length of the URL address is 99 characters. |
| CasFileURL | Specifies the name of the CAS file and the location of the server (IP address or FQDN) from which it is loaded. For example: http://server_name/file, https://server_name/file. Note: The maximum length of the URL address is 99 characters. |
| TLSRootFileUrl | Specifies the name of the TLS trusted root certificate file and the location URL from where it's downloaded. |
| TLSCertFileUrl | Specifies the name of the TLS certificate file and the location URL from where it's downloaded. |
| UserInfoFileURL | Specifies the name of the User Information file and the location of the server (IP address or FQDN) from which it is loaded. For example: http://server_name/file, https://server_name/file. Note: The maximum length of the URL address is 99 characters. |
| AutoUpdateCmpFile | Enables / disables the Automatic Update mechanism for the cmp file. <ul style="list-style-type: none"> [0] = The Automatic Update mechanism doesn't apply to the cmp file (default). [1] = The Automatic Update mechanism includes the cmp file. |
| AutoUpdateFrequency | Determines the number of minutes the gateway waits between automatic updates. The default value is 0 (the update at fixed intervals mechanism is disabled). |
| AutoUpdatePredefinedTime | Schedules an automatic update to a predefined time of the day. The range is 'HH:MM' (24-hour format). For example: 20:18 Note: The actual update time is randomized by five minutes to reduce the load on the Web servers. |
| ResetNow | This parameter is now obsolete. |
| BootP and TFTP Parameters | |
| The BootP parameters are special 'Hidden' parameters. Once defined and saved in the flash memory, they are used even if they don't appear in the <i>ini</i> file. | |
| BootPRetries | Note: This parameter only takes effect from the next reset of the gateway. This parameter is used to: |

Table 6-2: System Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description | |
|--|---|--|
| | <p>Set the number of BootP requests the gateway sends during start-up. The gateway stops sending BootP requests when either BootP reply is received or number of retries is reached.</p> <ul style="list-style-type: none"> ▪ [1] = 1 BootP retry, 1 sec. ▪ [2] = 2 BootP retries, 3 sec. ▪ [3] = 3 BootP retries, 6 sec. (default). ▪ [4] = 10 BootP retries, 30 sec. ▪ [5] = 20 BootP retries, 60 sec. ▪ [6] = 40 BootP retries, 120 sec. ▪ [7] = 100 BootP retries, 300 sec. ▪ [15] = BootP retries indefinitely. | <p>Set the number of DHCP packets the gateway sends. After all packets were sent, if there's still no reply, the gateway loads from flash.</p> <ul style="list-style-type: none"> ▪ [1] = 4 DHCP packets ▪ [2] = 5 DHCP packets ▪ [3] = 6 DHCP packets (default) ▪ [4] = 7 DHCP packets ▪ [5] = 8 DHCP packets ▪ [6] = 9 DHCP packets ▪ [7] = 10 DHCP packets ▪ [15] = 18 DHCP packets |
| BootPSelectiveEnable | <p>Enables the Selective BootP mechanism.</p> <ul style="list-style-type: none"> ▪ [1] = Enabled. ▪ [0] = Disabled (default). <p>The Selective BootP mechanism (available from Boot version 1.92) enables the gateway's integral BootP client to filter unsolicited BootP/DHCP replies (accepts only BootP replies that contain the text 'AUDC' in the vendor specific information field). This option is useful in environments where enterprise BootP/DHCP servers provide undesired responses to the gateway's BootP requests.</p> <p>Note: When working with DHCP (DHCPEnable = 1) the selective BootP feature must be disabled.</p> | |
| BootPDelay | <p>The interval between the device's startup and the first BootP/DHCP request that is issued by the device.</p> <ul style="list-style-type: none"> ▪ [1] = 1 second (default). ▪ [2] = 3 second. ▪ [3] = 6 second. ▪ [4] = 30 second. ▪ [5] = 60 second. <p>Note: This parameter only takes effect from the next reset of the device.</p> | |

Table 6-2: System Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| ExtBootPReqEnable | <ul style="list-style-type: none"> ▪ [0] = Disable (default). ▪ [1] = Enable extended information to be sent in BootP request. <p>If enabled, the device uses the vendor specific information field in the BootP request to provide device-related initial startup information such as blade type, current IP address, software version, etc. For a full list of the vendor specific Information fields, refer to the <i>SIP Series Reference Manual</i>.</p> <p>The BootP/TFTP configuration utility displays this information in the 'Client Info' column (refer to the <i>SIP Series Reference Manual</i>).</p> <p>Note: This option is not available on DHCP servers.</p> |
| Serial Parameters | |
| DisableRS232 | <ul style="list-style-type: none"> ▪ [0] = RS-232 serial port is enabled (default). ▪ [1] = RS-232 serial port is disabled. <p>The RS-232 serial port can be used to change the networking parameters (refer to Assigning an IP Address Using the CLI on page 53) and view error / notification messages.</p> <p>For information on establishing a serial communications link with the gateway, refer to Accessing the CLI on page 53.</p> |
| SerialBaudRate | <p>Determines the value of the RS-232 baud rate.</p> <p>The valid range is any value. It is recommended to use the following standard values: 1200, 2400, 9600 (default), 14400, 19200, 38400, 57600, 115200.</p> |
| SerialData | <p>Determines the value of the RS-232 data bit.</p> <ul style="list-style-type: none"> ▪ [7] = 7-bit. ▪ [8] = 8-bit (default). |
| SerialParity | <p>Determines the value of the RS-232 polarity.</p> <ul style="list-style-type: none"> ▪ [0] = None (default). ▪ [1] = Odd. ▪ [2] = Even. |
| SerialStop | <p>Determines the value of the RS-232 stop bit.</p> <ul style="list-style-type: none"> ▪ [1] = 1-bit (default). ▪ [2] = 2-bit. |
| SerialFlowControl | <p>Determines the value of the RS-232 flow control.</p> <ul style="list-style-type: none"> ▪ [0] = None (default). ▪ [1] = Hardware. |

6.5.3 Web and Telnet Parameters

Table 6-3: Web and Telnet Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| WebAccessList_x | <p>Defines up to ten IP addresses that are permitted to access the gateway's Embedded Web Server and Telnet interfaces. Access from an undefined IP address is denied. This security feature is inactive (the gateway can be accessed from any IP address) when the table is empty. For example:</p> <p>WebAccessList_0 = 10.13.2.66 WebAccessList_1 = 10.13.77.7</p> <p>The default value is 0.0.0.0 (the gateway can be accessed from any IP address). For defining the Web and Telnet Access list using the Embedded Web Server, refer to 'Configuring the Web and Telnet Access List' on page 225.</p> |
| WebRADIUSLogin | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232 . |
| DisableWebTask | <ul style="list-style-type: none"> ▪ [0] = Enable Web management (default). ▪ [1] = Disable Web management. |
| ResetWebPassword | <p>Resets the username and password of the primary and secondary accounts to their defaults.</p> <ul style="list-style-type: none"> ▪ [0] = Password and username retain their values (default). ▪ [1] = Password and username are reset (for the default username and password, refer to 'User Accounts' on page 58). <p>Note: The username and password cannot be reset from the Embedded Web Server (i.e., via AdminPage or by loading an <i>ini</i> file).</p> |

Table 6-3: Web and Telnet Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| WelcomeMessage | <p>Configures the Welcome message that appears after a Embedded Web Server login.</p> <p>The format of this <i>ini</i> file parameter table is:</p> <pre>[WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text WelcomeMessage 1 = "..."; WelcomeMessage 2 = "..."; WelcomeMessage 3 = "..."; [WelcomeMessage]</pre> <p>For Example:</p> <pre>[WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text WelcomeMessage 1 = "*****"; WelcomeMessage 2 = "***** This is a Welcome message *****"; WelcomeMessage 3 = "*****"; [WelcomeMessage]</pre> <p>Notes:</p> <ul style="list-style-type: none"> Each index represents a line of text in the Welcome message box. Up to 20 indexes can be defined. If this parameter is not configured, no Welcome message box is displayed. |
| DisableWebConfig | <ul style="list-style-type: none"> [0] = Enable changing parameters from Embedded Web Server (default). [1] = Operate Embedded Web Server in 'read only' mode. |
| HTTPport | HTTP port used for Web management (default is 80). |
| Telnet Parameters | |
| TelnetServerEnable | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |
| TelnetServerPort | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |
| TelnetServerIdleDisconnect | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |
| SSHServerEnable | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |
| SSHServerPort | For a description of this parameter, refer to 'Configuring the Application Settings' on page 182. |

Table 6-3: Web and Telnet Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|--|
| Customizing the Web Appearance Parameters For detailed information on customizing the Embedded Web Server interface, refer to 'Customizing the Web Interface' on page 65. | |
| UseProductName | Determines whether the UserProductName text string is displayed instead of the default product name. <ul style="list-style-type: none"> ▪ [0] = Disabled (default). ▪ [1] = Enables the display of the user-defined UserProductName text string (in the Embedded Web Server interface and in the extracted <i>ini</i> file). If enabled, the UserProductName text string is displayed instead of the default product name. |
| UserProductName | Text string that replaces the default product name that appears in the Embedded Web Server (upper right-hand corner) and the extracted <i>ini</i> file. The default is 'Mediant 1000'. The string can be up to 29 characters. |
| UseWebLogo | <ul style="list-style-type: none"> ▪ [0] = Logo image is used (default). ▪ [1] = Text string is used instead of a logo image. If enabled, AudioCodes' default logo (or any other logo defined by the LogoFileName parameter) is replaced with a text string defined by the WebLogoText parameter. |
| WebLogoText | Text string that replaces the logo image. The string can be up to 15 characters. |
| LogoWidth | Width (in pixels) of the logo image. Note: The optimal setting depends on the resolution settings. The default value is 441, which is the width of AudioCodes' displayed logo. |
| LogoFileName | Name of the image file (of type GIF, JPEG, or JPG) containing the user's logo. File name can be up to 47 characters. The logo file name can be used to replace AudioCodes' default Web logo with a user defined logo. |
| BkgImageFileName | Name of the file containing the user's background image (of file type GIF, JPEG, or JPG). File name can be up to 47 characters. The background file can be used to replace AudioCodes' default background image with a user defined background. |

6.5.4 Security Parameters

Table 6-4: Security Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|--|
| EnableIPSec | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232 . |
| EnableMediaSecurity | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232 . |
| MediaSecurityBehaviour | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232 . |
| EnableSIPS | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| TLSVersion | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232 . |
| TLSTLSLocalSIPPort | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| SIPSRequireClientCertificate | <ul style="list-style-type: none"> ▪ [0] = The gateway doesn't require client certificate (default). ▪ [1] = The gateway (when acting as a server for the TLS connection) requires reception of client certificate to establish the TLS connection. <p>Note: The SIPS certificate files can be changed using the parameters HTTPSCertFileName and HTTPSRootFileName.</p> |
| Secure Hypertext Transport Protocol (HTTPS) Parameters | |
| HTTPSOnly | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232 . |
| HTTPSPort | Determine the local Secured HTTPS port of the device. The valid range is 1 to 65535 (other restrictions may apply within this range). The default port is 443. |
| HTTPSCipherString | Defines the Cipher string for HTTPS (in OpenSSL cipher list format). Refer to URL http://www.openssl.org/docs/apps/ciphers.html . The range is EXP, RC4. Default is 0. |
| WebAuthMode | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232 . |
| HTTPSRequireClientCertificate | Requires client certificates for HTTPS connection. The client certificate must be preloaded to the gateway, and its matching private key must be installed on the managing PC. Time and date must be correctly set on the gateway, for the client certificate to be verified. <ul style="list-style-type: none"> ▪ [0] = Client certificates are not required (default). ▪ [1] = Client certificates are required. |

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| HTTPSRootFileName | Defines the name of the HTTPS trusted root certificate file to be loaded via TFTP. The file must be in base64-encoded PEM (Privacy Enhanced Mail) format. The valid range is a 47-character string. Note: This parameter is only relevant when the gateway is loaded via BootP/TFTP. For information on loading this file via the Embedded Web Server, refer to the <i>SIP Series Reference Manual</i> . |
| HTTPSPkeyFileName | Defines the name of a private key file (in unencrypted PEM format) to be loaded from the TFTP server. |
| HTTPSCertFileName | Defines the name of the HTTPS server certificate file to be loaded via TFTP. The file must be in base64-encoded PEM format. The valid range is a 47-character string. Note: This parameter is only relevant when the gateway is loaded via BootP/TFTP. For information on loading this file via the Embedded Web Server, refer to the <i>SIP Series Reference Manual</i> . |
| VoiceMenuPassword | For a description of this parameter, refer to Configuring the General Security Settings on page 232 . |
| Internal Firewall Parameters | |
| AccessList_Source_IP | For a description of this parameter, refer to 'Configuring the Firewall Settings' on page 226 . |
| AccessList_Net_Mask | For a description of this parameter, refer to 'Configuring the Firewall Settings' on page 226 . |
| AccessList_Start_Port AccessList_End_Port | For a description of this parameter, refer to 'Configuring the Firewall Settings' on page 226 . |
| AccessList_Protocol | For a description of this parameter, refer to 'Configuring the Firewall Settings' on page 226 . |
| AccessList_Packet_Size | For a description of this parameter, refer to 'Configuring the Firewall Settings' on page 226 . |
| AccessList_Byte_Rate | For a description of this parameter, refer to 'Configuring the Firewall Settings' on page 226 . |
| AccessList_Byte_Burst | For a description of this parameter, refer to 'Configuring the Firewall Settings' on page 226 . |
| AccessList_Allow_Type | For a description of this parameter, refer to 'Configuring the Firewall Settings' on page 226 . |
| AccessList_MatchCount | For a description of this parameter, refer to 'Configuring the Firewall Settings' on page 226 . |

6.5.5 RADIUS Parameters

For detailed information on the supported RADIUS attributes, refer to 'Supported RADIUS Attributes' on page 402.

Table 6-5: RADIUS Parameter

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| EnableRADIUS | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232. |
| AAAIindications | For a description of this parameter, refer to 'Configuring RADIUS Accounting Parameters' on page 166. |
| MaxRADIUSSessions | Number of concurrent calls that can communicate with the RADIUS server (optional). The valid range is 0 to 240. The default value is 240. |
| SharedSecret | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232. |
| RADIUSRetransmission | Number of retransmission retries. The valid range is 1 to 10. The default value is 3. |
| RadiusTO | Determines the time interval (measured in seconds) the gateway waits for a response before a RADIUS retransmission is issued. The valid range is 1 to 30. The default value is 10. |
| RADIUSAuthServerIP | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232. |
| RADIUSAuthPort | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232. |
| RADIUSAccServerIP | For a description of this parameter, refer to 'Configuring RADIUS Accounting Parameters' on page 166. |
| RADIUSAccPort | For a description of this parameter, refer to 'Configuring RADIUS Accounting Parameters' on page 166. |
| RadiusAccountingType | For a description of this parameter, refer to 'Configuring RADIUS Accounting Parameters' on page 166. |
| DefaultAccessLevel | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232. |
| RadiusLocalCacheMode | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232. |
| RadiusLocalCacheTimeout | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232. |
| RadiusVSAVendorID | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232. |
| RadiusVSAAccessAttribute | For a description of this parameter, refer to 'Configuring the General Security Settings' on page 232. |

6.5.6 SNMP Parameters

Table 6-6: SNMP Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| DisableSNMP | For a description of this parameter, refer to 'Configuring the Management Settings' on page 243. |
| SNMPPort | The device's local UDP port used for SNMP Get/Set commands. The range is 100 to 3999. The default port is 161. |
| SNMPTrustedMGR_x | Up to five IP addresses of remote trusted SNMP managers from which the SNMP agent accepts and processes get and set requests. Notes: <ul style="list-style-type: none"> If no values are assigned to these parameters any manager can access the device. Trusted managers can work with <i>all</i> community strings. |
| ChassisPhysicalAlias | This object is an 'alias' name for the physical entity as specified by a network manager, and provides a non-volatile 'handle' for the physical entity. The valid range is a string of up to 255 characters. |
| ChassisPhysicalAssetID | This object is a user-assigned asset tracking identifier for the Mediant 1000 chassis as specified by an EMS, and provides non-volatile storage of this information. The valid range is a string of up to 255 characters. |
| ifAlias | The textual name of the interface. The value is equal to the ifAlias SNMP MIB object. The valid range is a string of up to 64 characters. |
| KeepAliveTrapPort | The port to which the keep-alive traps are sent. The valid range is 0 - 65534. The default is port 162. |
| SendKeepAliveTrap | When enabled, this parameter invokes the keep-alive trap and sends it every 9/10 of the time defined in the parameter defining NAT Binding Default Timeout. <ul style="list-style-type: none"> [0] = Disable [1] = Enable |
| SNMPSysOid | Defines the base product system OID. Default is eSNMP_AC_PRODUCT_BASE_OID_D. |
| SNMPTrapEnterpriseOid | Defines a Trap Enterprise OID. Default is eSNMP_AC_ENTERPRISE_OID. The inner shift of the trap in the AcTrap subtree is added to the end of the OID in this parameter. |
| acUserInputAlarmDescription | Defines the description of the input alarm. |
| acUserInputAlarmSeverity | Defines the severity of the input alarm. |

Table 6-6: SNMP Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| AlarmHistoryTableMaxSize | Determines the maximum number of rows in the Alarm History table. The parameter can be controlled by the Config Global Entry Limit MIB (located in the Notification Log MIB). The valid range is 50 to 1000. The default value is 500. |
| SNMP Trap Parameters | |
| SNMPManagerTableIP_x | For a description of this parameter, refer to 'Configuring the SNMP Managers Table' on page 246 . |
| SNMPManagerTrapPort_x | For a description of this parameter, refer to 'Configuring the SNMP Managers Table' on page 246 . |
| SNMPManagerTrapUser_x | This parameter can be set to the name of any configured SNMPV3 user to associate with this trap destination. This determines the trap format, authentication level, and encryption level. By default, the trap is associated with the SNMP trap community string. |
| SNMPManagerIsUsed_x | For a description of this parameter, refer to 'Configuring the SNMP Managers Table' on page 246 . |
| SNMPManagerTrapSendingEnable_x | For a description of this parameter, refer to 'Configuring the SNMP Managers Table' on page 246 . |
| SNMPTrapManagerHostName | For a description of this parameter, refer to 'Configuring the Management Settings' on page 243 . |
| SNMP Community String Parameters | |
| SNMPReadOnlyCommunityString_x | For a description of this parameter, refer to 'Configuring the SNMP Community Strings' on page 248 . |
| SNMPReadWriteCommunityString_x | For a description of this parameter, refer to 'Configuring the SNMP Community Strings' on page 248 . |
| SNMPTrapCommunityString | For a description of this parameter, refer to 'Configuring the SNMP Community Strings' on page 248 . |
| SNMP v3 Users Parameters | |
| SNMPUsers_Index | For a description of this parameter, refer to 'Configuring SNMP V3 Users' on page 249 . |
| SNMPUsers_Username | For a description of this parameter, refer to 'Configuring SNMP V3 Users' on page 249 . |
| SNMPUsers_AuthProtocol | For a description of this parameter, refer to 'Configuring SNMP V3 Users' on page 249 . |
| SNMPUsers_PrivProtocol | For a description of this parameter, refer to 'Configuring SNMP V3 Users' on page 249 . |
| SNMPUsers_AuthKey | For a description of this parameter, refer to 'Configuring SNMP V3 Users' on page 249 . |
| SNMPUsers_PrivKey | For a description of this parameter, refer to 'Configuring SNMP V3 Users' on page 249 . |
| SNMPUsers_Group | For a description of this parameter, refer to 'Configuring SNMP V3 Users' on page 249 . |

6.5.7 SIP Configuration Parameters

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| SIPTransportType | For a description of this parameter, refer to 'General Parameters' on page 72. |
| TCPLocalSIPPort | For a description of this parameter, refer to 'General Parameters' on page 72. |
| SIPDestinationPort | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnableTCPConnectionReuse | For a description of this parameter, refer to 'General Parameters' on page 72. |
| SIPTCPTimeout | For a description of this parameter, refer to 'General Parameters' on page 72. |
| LocalSIPPort | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnableFaxReRouting | For a description of this parameter, refer to 'General Parameters' on page 103. |
| SIPGatewayName | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| IsProxyUsed | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| ProxyIP | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| ProxyIP ProxyIP ProxyIP | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| ProxyName | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| EnableProxySRVQuery | This parameter is obsolete; use the parameter ProxyDNSQueryType. |
| EnableSRVQuery | This parameter is obsolete; use the parameter DNSQueryType. |
| AlwaysSendToProxy | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| SendInviteToProxy | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| PreferRouteTable | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| EnableProxyKeepAlive | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| ProxyKeepAliveTime | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| DNSQueryType | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| ProxyDNSQueryType | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| UseSIPTrgp | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnableGRUU | For a description of this parameter, refer to 'General Parameters' on page 72. |
| UserAgentDisplayInfo | For a description of this parameter, refer to 'General Parameters' on page 72. |
| SIPSDPSessionOwner | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnableRTCPAttribute | Enables or disables the use of the 'rtcp' attribute in the outgoing SDP. <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = Enable (default) |
| UseGatewayNameForOptions | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| IsProxyHotSwap | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| ProxyHotSwapRtx | This parameter is now obsolete; use instead HotSwapRtx. |
| HotSwapRtx | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| ProxyRedundancyMode | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| ProxyLoadBalancingMethod | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| ProxyIPListRefreshTime | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| IsFallbackUsed | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| UserName | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| Password | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| Cnonce | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| SIPChallengeCachingMode | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| MutualAuthenticationMode | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| IsRegisterNeeded | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| RegistrarIP | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| RegistrarName | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| GWRegistrationName | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| AuthenticationMode | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| OOSOnRegistrationFail | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| RegistrationTime | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| RegistrationTimeDivider | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| RegistrationRetryTime | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| RegisterOnInviteFailure | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| RegistrationTimeThreshold | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| NumberOfActiveDialogs | Defines the maximum number of active SIP dialogs that are not call related (i.e., REGISTER and SUBSCRIBE). This parameter is used to control the Registration / Subscription rate. The valid range is 1 to 20. The default value is 20. |
| PrackMode | For a description of this parameter, refer to 'General Parameters' on page 72. |
| AssertedIdMode | For a description of this parameter, refer to 'General Parameters' on page 72. |
| PAssertedUserName | Defines a 'representative number' (up to 50 characters) that is used as the User Part of the Request-URI in the P-Asserted-Id header of an outgoing INVITE (for Tel-to-IP calls). The default value is NULL. |
| UseAORInReferToHeader | Defines the source for the SIP URI set in the Refer-to header of outgoing REFER messages. <ul style="list-style-type: none"> ▪ [0] = Use SIP URI from Contact header (default) of the initial call. ▪ [1] = Use SIP URI from To/From header of the initial call. |
| UseTelURIForAssertedID | For a description of this parameter, refer to 'General Parameters' on page 72. |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| EnableRPIheader | For a description of this parameter, refer to 'General Parameters' on page 72. |
| IsUserPhone | For a description of this parameter, refer to 'General Parameters' on page 72. |
| IsUserPhoneInFrom | For a description of this parameter, refer to 'General Parameters' on page 72. |
| IsUseToHeaderAsCalledNumber | <ul style="list-style-type: none"> ▪ [0] = Sets the destination number to the user part of the Request-URI for IP-to-Tel calls, and sets the 'Contact' header to the source number for Tel-to-IP calls (default). ▪ [1] = Sets the destination number to the user part of the 'To' header for IP-to-Tel calls, and sets the 'Contact' header to the username parameter for Tel-to-IP calls. |
| EnableHistoryInfo | For a description of this parameter, refer to 'General Parameters' on page 72. |
| SIPSubject | For a description of this parameter, refer to 'General Parameters' on page 72. |
| MultiPtimeFormat | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnableReasonHeader | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnableSemiAttendedTransfer | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnablePtime | <ul style="list-style-type: none"> ▪ [0] = Remove the ptime header from SDP. ▪ [1] = Include the ptime header in SDP (default). |
| EnableUserInfoUsage | For a description of this parameter, refer to 'General Parameters' on page 103. |
| EnableRport | <p>Enables / disables the usage of the 'rport' parameter in the Via header.</p> <ul style="list-style-type: none"> ▪ [0] = Enabled. ▪ [1] = Disabled (default). <p>The gateway adds an 'rport' parameter to the Via header field of each outgoing SIP message. The first Proxy that receives this message sets the 'rport' value of the response to the actual port from which the request was received. This method is used, for example, to enable the gateway to identify its port mapping outside a NAT.</p> <p>If the Via doesn't include 'rport' tag, the destination port of the response is taken from the host part of the VIA.</p> <p>If the Via includes 'rport' tag without port value, the destination port of the response is the source port of the incoming request.</p> <p>If the Via includes 'rport' tag with a port value (rport=1001), the destination port of the response is the port indicated in the 'rport' tag.</p> |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| VBRCoderHeaderFormat | <p>Defines the format of the RTP header for VBR coders.</p> <ul style="list-style-type: none"> ▪ [0] = Payload only (no header, no TOC, no m-factor) -- similar to RFC 3558 Header Free format (default). ▪ [1] = Supports RFC 2658 - 1 byte for interleaving header (always 0), TOC, no m-factor. ▪ [2] = Payload including TOC only, allow m-factor. ▪ [3] = RFC 3558 Interleave/Bundled format. |
| TransparentCoderOnData Call | <ul style="list-style-type: none"> ▪ [0] = Only use coders from the coder list (default). ▪ [1] = Use transparent coder for data calls (according to RFC 4040). <p>The 'Transparent' coder can be used on data calls. When the gateway receives a Setup message from the ISDN with 'TransferCapabilities = data', it can initiate a call using the coder 'Transparent' (even if the coder is not included in the coder list).</p> <p>The initiated INVITE includes the following SDP attribute: a=rtpmap:97 CLEARMODE/8000</p> <p>The default Payload Type is set according to the CoderName table. If the Transparent coder is not set in the Coders table, the default value is set to 56. The Payload Type is negotiated with the remote side, i.e., the selected Payload Type is according to the remote side selection.</p> <p>The receiving gateway must include the 'Transparent' coder in its coder list.</p> |
| IsFaxUsed | For a description of this parameter, refer to 'General Parameters' on page 72 . |
| T38UseRTPPort | <p>Defines that the T.38 packets are sent / received using the same port as RTP packets.</p> <ul style="list-style-type: none"> ▪ [0] = Use the RTP port +2 to send / receive T.38 packets (default). ▪ [1] = Use the same port as the RTP port to send / receive T.38 packets. |
| DefaultReleaseCause | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| IPAlertTimeout | For a description of this parameter, refer to 'General Parameters' on page 72 . |
| SIPPSessionExpires | For a description of this parameter, refer to 'General Parameters' on page 72 . |
| SessionExpiresMethod | For a description of this parameter, refer to 'General Parameters' on page 72 . |
| MINSE | For a description of this parameter, refer to 'General Parameters' on page 72 . |
| SIPMaxRtx | For a description of this parameter, refer to 'General Parameters' on page 72 . |
| SipT1Rtx | For a description of this parameter, refer to 'General Parameters' on page 72 . |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| SipT2Rtx | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnableEarlyMedia | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnableTransfer | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| XferPrefix | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| EnableHold | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| EnableForward | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| CallWaitingPerPort | <p>Defines call waiting per port. [CallWaitingPerPort] FORMAT CallWaitingPerPort_Index = CallWaitingPerPort_IsEnabled; CallWaitingPerPort_Port, CallWaitingPerPort_Module; [CallWaitingPerPort]</p> <p>Where,</p> <ul style="list-style-type: none"> IsEnabled = enables [1] or disables [0] call waiting Port = Port number Module = Module number <p>For example: [CallWaitingPerPort] CallWaitingPerPort 0 = 0,1,1\$\$; CallWaitingPerPort 1 = 1,2,1\$\$; [CallWaitingPerPort]</p> <p>If enabled, when an FXS gatewaymodule receives a call on a busy endpoint, it responds with a 182 response (and not with a 486 busy). The gateway plays a call waiting indication signal. When hook-flash is detected, the gateway switches to the waiting call. The gateway that initiated the waiting call plays a Call Waiting Ringback tone to the calling party after a 182 response is received.</p> <p>Notes:</p> <ul style="list-style-type: none"> If this parameter is not configured (default), use the global parameter EnableCallWaiting (refer to Supplementary Services on page 113). The numbering of channels starts with 0. The gateway's Call Progress Tones file must include a 'call waiting Ringback' tone (caller side) and a 'call waiting' tone (called side, FXS only). The 'Enable Hold' parameter must be enabled on both the calling and the called sides. To define call waiting using the Embedded Web Server, refer to Call Waiting on page 418. |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| CHRRTimeout | For a description of this parameter, refer to Supplementary Services on page 113. |
| EnableCallWaiting | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| 3WayConferenceMode | <p>Defines the mode of operation when the 3-Way Conference feature is used.</p> <ul style="list-style-type: none"> ▪ [0] = Conference-initiating INVITE (sent by the gateway), uses the ConferenceID concatenated with a unique identifier as the Request-UR (default). ▪ [1] = Conference-initiating INVITE (sent by the gateway), uses only the ConferenceID as the Reques-URI. <p>If 3wayConferenceMode is set to 0, the Conference-initiating INVITE sent by the gateway, uses the ConferenceID concatenated with a unique identifier as the Request-URI. This same Request-URI is set as the Refer-To header value in the REFER messages that are sent to the two remote parties.</p> <p>If 3wayConferenceMode is set to 1, the Conference-initiating INVITE sent by the gateway, only uses the ConferenceID as the Reques-URI. The media server sets the Contact header of the 200 OK response to the actual unique identifier (Conference URI) to be used by the participants. This Conference URI is included (by the gateway), in the Refer-To header value in the REFER messages sent by the gateway to the remote parties. The remote parties join the conference by sending INVITE messages to the media server using this conference URI.</p> |
| Enable3WayConference | For a description of this parameter, refer to Supplementary Services on page 113. |
| ConferenceCode | For a description of this parameter, refer to Supplementary Services on page 113. |
| ConferenceID | For a description of this parameter, refer to Supplementary Services on page 113. |
| BipOnConference | <p>Determines whether a beep is played when a new participant joins a conference and when a participant leaves a conference (in the latter case, a beep of a different pitch is heard).</p> <ul style="list-style-type: none"> ▪ [0] = Beep is disabled. ▪ [1] = Beep is enabled (default). |
| Send180ForCallWaiting | <ul style="list-style-type: none"> ▪ [0] = Use 182 Queued response to indicate a call waiting (default). ▪ [1] = Use 180 Ringing response to indicate a call waiting. |
| HookFlashCode | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| UseSIPURIForDiversionHeader | <p>Sets the URI format in the Diversion header.</p> <ul style="list-style-type: none"> ▪ [0] = 'tel:' (default). ▪ [1] = 'sip:'. |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| WarningToneDuration | Defines the duration (in seconds) for which Off-Hook Warning Tone is played to the user. The valid range is -1 to 2,147,483,647 seconds. The default is 600 seconds. Note: A negative value indicates that the tone is played infinitely. |
| FirstCallWaitingToneID | Determines the index of the first Call Waiting Tone in the CPT file. This feature enables the called party to distinguish between four different call origins (e.g., external vs. internal calls). The gateway plays the tone received in the 'play tone CallWaitingTone#' parameter of an INFO message + the value of this parameter - 1. The valid range is -1 to 100. The default value is -1 (not used). Notes: <ul style="list-style-type: none"> It is assumed that all Call Waiting Tones are defined in sequence in the CPT file. This feature is relevant only to Broadsoft's application servers (the tone is played using INFO message). |
| RTPOnlyMode | For a description of this parameter, refer to 'General Parameters' on page 103. |
| TimeoutBetween100And18x | Defines the timeout (in msec) between receiving a 100 Trying response and a subsequent 18x response. If a 18x response is not received before this timer expires, the call is disconnected. The valid range is 0 to 32,000. The default value is 0 (i.e., no timeout). |
| TransparentCoderPresentation | Determines the format of Transparent coder representation in the SDP. Valid options include: <ul style="list-style-type: none"> [0] = clearmode (default) [1] = X-CCD |
| RxDTMFOption | For a description of this parameter, refer to 'DTMF & Dialing Parameters' on page 98. |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| TxDTMFOption | <p>Determines a single or several (up to 5) preferred transmit DTMF negotiation methods. Format of this <i>ini</i> file parameter table: [TxDTMFOption] FORMAT TxDTMFOption_Index = TxDTMFOption_Type; [TxDTMFOption]</p> <p>For example: [TxDTMFOption] TxDTMFOption 0 = 1; [TxDTMFOption]</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description of <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. DTMF negotiation methods are prioritized according to the order of their appearance. When out-of-band DTMF transfer is used ([1], [2], or [3]), the parameter DTMFTransportType is automatically set to 0 (DTMF digits are erased from the RTP stream). When RFC 2833 ([4]) is used, the gateway: <ol style="list-style-type: none"> 1) Negotiates RFC 2833 Payload Type (PT) using local and remote SDPs. 2) Sends DTMF packets using RFC 2833 PT according to the PT in the received SDP. 3) Expects to receive RFC 2833 packets with the same PT as configured by the parameter RFC2833PayloadType. 4) Uses the same PT for send and receive if the remote party doesn't include the RFC 2833 DTMF PT in its SDP. When TxDTMFOption is set to [0], the RFC 2833 PT is set according to the parameter RFC2833PayloadType for both transmit and receive. For defining this parameter using the Embedded Web Server, refer to 'DTMF & Dialing Parameters' on page 98. |
| DisableAutoDTMFmute | <p>Enables / disables the automatic mute of DTMF digits when out-of-band DTMF transmission is used.</p> <ul style="list-style-type: none"> [0] = Auto mute is used (default). [1] = No automatic mute of in-band DTMF. <p>When DisableAutoDTMFmute = 1, the DTMF transport type is set according to the parameter DTMFTransportType and the DTMF digits aren't muted if out-of-band DTMF mode is selected ('TxDTMFOption =1, 2 or 3'). This enables the sending of DTMF digits in-band (transparent of RFC 2833) in addition to out-of-band DTMF messages. Note: Usually this mode is not recommended.</p> |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| EnableImmediateTrying | Determines if and when the gateway sends a 100 Trying response to an incoming INVITE request. <ul style="list-style-type: none"> ▪ [0] = 100 Trying response is sent upon receipt of PROCEEDING message from the PSTN. ▪ [1] = 100 Trying response is sent immediately upon receipt of INVITE request (default). |
| EnableReasonHeader | For a description of this parameter, refer to 'General Parameters' on page 72. |
| 3xxBehavior | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnablePChargingVector | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EnableVMURI | For a description of this parameter, refer to 'General Parameters' on page 72. |
| MaxActiveCalls | For a description of this parameter, refer to 'General Parameters' on page 103. |
| MaxCallDuration | For a description of this parameter, refer to 'General Parameters' on page 103. |
| EnableBusyOut | For a description of this parameter, refer to 'General Parameters' on page 103. |
| EnableDigitDelivery2IP | For a description of this parameter, refer to 'General Parameters' on page 103. |
| EnableDigitDelivery | For a description of this parameter, refer to 'General Parameters' on page 103. |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| Authentication | <p>Defines a username and password combination for authenticating each gateway port. Format of this ini file parameter table: [Authentication] FORMAT Authentication_Index = Authentication_UserId, Authentication_UserPassword, Authentication_Port, Authentication_Module; [Authentication] Where,</p> <ul style="list-style-type: none"> ▪ UserId = User name ▪ UserPassword = Password ▪ Port = Port number ▪ Module = Module number (0 - 5) <p>For example: [Authentication] Authentication 1 = david,14325,1,0; Authentication 2 = Alex,18552,1,0; Authentication 3 = user1, 1234,1,0; [Authentication]</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For an explanation on ini file parameter tables, refer to Structure of ini File Parameter Tables on page 295. ▪ You can omit either the username or password using the sign '\$\$'. If omitted, the port's phone number is used for authentication. ▪ The indexing of this ini file parameter table starts at 1. ▪ To configure the authentication username and password using the Embedded Web Server, refer to Authentication on page 154. |
| SITDetectorEnable | <p>Enables or disables Special Information Tone (SIT) detection according to the ITU-T recommendation E.180/Q.35.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default). ▪ [1] = Enable. |
| EnableSAS | For a description of this parameter, refer to Stand-Alone Survivability on page 123 . |
| SASLocalSIPUDPPort | For a description of this parameter, refer to Stand-Alone Survivability on page 123 . |
| SASDefaultGatewayIP | For a description of this parameter, refer to Stand-Alone Survivability on page 123 . |
| SASRegistrationTime | <p>Determines the Expires header value that is returned in a 200 OK response to an incoming REGISTER message when in SAS 'Emergency Mode'. The valid range is or 10 (Digital) to 2,000,000. The default value is 20.</p> |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| Profile Parameters | |
| CoderName | <p>Defines the gateway's coder list ('Coders' table in the Embedded Web Server -- refer to 'Coders' on page 94), including up to 5 groups of coders (consisting of up to five coders per group) that can be associated with IP or Tel profiles ('Coder Group Settings' screen in the Embedded Web Server -- refer to 'Coder Group Settings' on page 145). The first group of coders (indices 0 through 4) is the default coder list and default coder group.</p> <p>[CoderName] FORMAT CoderName_Index = CoderName_Type, CoderName_PacketInterval, CoderName_rate, CoderName_PayloadType, CoderName_Sce; [CoderName]</p> <p>Where, Type = Coder name PacketInterval = Packetization time Rate = Packetization rate PayloadType = Payload type Sce = Silence suppression mode</p> <p>For example: [CoderName] CoderName 0 = g711Alaw64k, 20,,,0; CoderName 1 = g726, \$\$, 3, 38, 0; CoderName 2 = g729, 40, 255, 255, 1; [CoderName]</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description of using <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. The coder name is case-sensitive. For a list of supported coders, refer to 'Coders' on page 94. If silence suppression is not defined for a specific coder, the value defined by the parameter EnableSilenceCompression is used. The value of several fields is hard-coded according to common standards (e.g., payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored. Only the ptime of the first coder in the defined coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined. If the coder G.729 is selected and silence suppression is enabled (for this coder), the gateway includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception is when the remote gateway is a Cisco device (IsCiscoSCEMode). CoderName can appear up to 25 times (five coders in five coder groups). |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| IPProfile | <p>Configures the IP profiles table (for Embedded Web Server, refer to 'IP Profile Settings' on page 148). [IPProfile] FORMAT IPProfile_Index = IPProfile_ProfileName, IPProfile_IpPreference, IPProfile_CodersGroupID, IPProfile_IsFaxUsed*, IPProfile_JitterBufMinDelay*, IPProfile_JitterBufOptFactor*, IPProfile_IPDiffServ*, IPProfile_SigIPDiffServ*, N/A, IPProfile_RTPRedundancyDepth, IPProfile_RemoteBaseUDPPort, IPProfile_CNMode, IPProfile_VxxTransportType, IPProfile_NSEMode, N/A, IPProfile_PlayRBTone2IP, IPProfile_EnableEarlyMedia*, IPProfile_ProgressIndicator2IP*, IPProfile_ECE*; [IPProfile]</p> <p>* = Indicates common parameters used in both IP and Tel profiles. IpPreference = determines the priority of the Profile (1 to 20, where 20 is the highest preference). If both IP and Tel profiles apply to the same call, the coders and other common parameters (indicated with an asterisk) of the preferred Profile are applied to that call. If the Tel and IP profiles are identical, the Tel Profile parameters are applied.</p> <p>For example: [IPProfile] IPProfile_1 = name1,2,1,0,10,13,15,44,1,1,6000,0,2,0,0,0,1,0,1; IPProfile_2 = name2,\$;\$ [IPProfile]</p> <p>Notes:</p> <ul style="list-style-type: none"> ■ For a description of using <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. ■ Two adjacent dollar signs ('\$') indicate that the parameter's default value is used. ■ IPProfile can be used in the Tel to IP Routing and IP to Trunk Group Routing tables (Prefix and PSTNPrefix parameters). ■ The 'Profile Name' assigned to a Profile index, must enable users to identify it intuitively and easily. ■ This parameter can appear up to 9 times (i.e., index = 1 to 9). |

Table 6-7: SIP Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| TelProfile | <p>Configures the Tel Profile Settings table (refer to 'Tel Profile Settings' on page 146).</p> <p>[TelProfile]</p> <p>FORMAT TelProfile_Index = TelProfile_ProfileName, TelProfile_TelPreference, TelProfile_CodersGroupID, TelProfile_IsFaxUsed*, TelProfile_JitterBufMinDelay*, TelProfile_JitterBufOptFactor*, TelProfile_IPDiffServ*, TelProfile_SigIPDiffServ*, TelProfile_DtmfVolume, TelProfile_InputGain, TelProfile_VoiceVolume, TelProfile_EnableReversePolarity, TelProfile_EnableCurrentDisconnect, TelProfile_EnableDigitDelivery, TelProfile_EnableEC, TelProfile_MWIAAnalog, TelProfile_MWIDisplay, TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia*, TelProfile_ProgressIndicator2IP*, TelProfile_TimeForReorderTone*;</p> <p>[TelProfile]</p> <p>* = Indicates common parameters used in both IP and Tel profiles.</p> <p>TelPreference = determines the priority of the Profile (1 to 20, where 20 is the highest preference). If both IP and Tel profiles apply to the same call, the coders and other common parameters (indicated with an asterisk) of the preferred Profile are applied to that call. If the preference of the Tel and IP profiles is identical, the Tel Profile parameters are applied.</p> <p>For example:</p> <p>[TelProfile]</p> <p>TelProfile 1 = FaxProfile,1,1,1,40,13,22,33,\$,\$,\$,\$,0,0,0,1,0,0,\$,\$,0,\$\$;</p> <p>TelProfile 2 = ModemProfile,2,2,0,40,13,\$,\$,\$,\$,\$,\$,\$,\$,\$,\$,0,0,0,\$\$,0,\$\$;</p> <p>[TelProfile]</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description of using <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. Two adjacent dollar signs ('\$') indicates that the parameter's default value is used. The TelProfile index can be used in the Trunk Group table (TrunkGroup parameter). The 'Profile Name' assigned to a Profile index must enable users to identify it intuitively and easily. This parameter can appear up to 9 times (i.e., index = 1 to 9). |

6.5.8 Media Server Parameters

Table 6-8: IPmedia Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| MSCMLID | For a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page 175. |
| AmsProfile | Must be set to 1 to use advanced audio. |
| AASPackagesProfile | Must be set to 3 to use advanced audio. |
| AmsPrimaryLanguage | Determines the primary language used in the advanced audio package. The default value is "eng". The languages are according to ISO standard 639-2 language codes. |
| AmsSecondaryLanguage | Determines the secondary language used in the advanced audio package. The default value is "heb". The languages are according to ISO standard 639-2 language codes. |
| AMSAllowUrlAsAlias | <p>Determines whether or not play requests for remote URLs are first verified with local audio segments to determine if any have an alias matching for the URL. If a match is found, the corresponding local audio segment is played.</p> <ul style="list-style-type: none"> ▪ [0] = Always use remote storage (default). ▪ [1] = Check local storage first. <p>One application for this capability is that of a 'provisioned' cache within the gateway. For details on provisioning an alias and other audio provisioning capabilities, refer to the Audio Provisioning Server (APS) User's Manual.</p> |
| VoiceStreamUploadMethod | <p>Defines the HTTP request type for loading the voice stream to the file server.</p> <ul style="list-style-type: none"> ▪ [0] = POST (default). ▪ [1] = PUT. <p>Note: Applicable only to MSCML recording.</p> |
| APSEnabled | <p>Indicates whether Voice Prompt index references refer to audio provided by the Audio Provisioning Server (APS), or by the local Voice Prompts file.</p> <ul style="list-style-type: none"> ▪ [0] = APS disabled. Local Voice Prompts file is used. An audio reference in a play request (such as http://localhost/0) indicates that the Voice Prompt at index 0 in the Voice Prompts file is played. ▪ [1] = APS enabled (default). An audio reference (such as http://localhost/99) indicates that the audio segment provisioned on the APS with segment ID 99 is played. |
| NetAnnAnncID | For a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page 175. |
| EnableVoiceStreaming | For a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page 175. |
| VoiceStreamUploadPostURI | Defines the URI used on the POST request to upload voice data from the media server to a Web server. |

Table 6-8: IPmedia Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| MediaChannels | For a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page 175. |
| ConferenceID | For a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page 175. |
| BipOnConference | For a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page 175. |
| TranscodingID | For a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page 175. |
| ActiveSpeakersNotificationMinInterval | For a description of this parameter, refer to 'Configuring the IPmedia Settings' on page 202. |
| EnableAGC | For a description of this parameter, refer to 'Configuring the IPmedia Settings' on page 202. |
| AGCGainSlope | For a description of this parameter, refer to 'Configuring the IPmedia Settings' on page 202. |
| AGCRedirection | For a description of this parameter, refer to 'Configuring the IPmedia Settings' on page 202. |
| AGCTargetEnergy | For a description of this parameter, refer to 'Configuring the IPmedia Settings' on page 202. |
| EnableConferenceDTMFClamp | For a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page 175 |
| EnableConferenceDTMFReporting | For a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page 175 |

6.5.9 Voice Mail Parameters

For detailed information on the Voice Mail (VM) application, refer to the *CPE Configuration Guide for Voice Mail*.

Table 6-9: Voice Mail Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| VoiceMailInterface | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| SubscriptionMode | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| LineTransferMode | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| WaitForDialTime | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |

Table 6-9: Voice Mail Configuration Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|---|
| MWONCode | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| MWOffCode | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| MWISuffixCode | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| Digit Patterns The following digit pattern parameters apply only to VM applications that use the DTMF communication method. For the available pattern syntaxes, refer to the CPE Configuration Guide for Voice Mail. | |
| DigitPatternForwardOn Busy | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| DigitPatternForwardOn NoAnswer | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| DigitPatternForwardOn DND | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| DigitPatternForwardNo Reason | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| DigitPatternForwardOn BusyExt | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| DigitPatternForwardOn NoAnswerExt | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| DigitPatternForwardOn DNDExt | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| DigitPatternForwardNo ReasonExt | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| DigitPatternInternalCall | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| DigitPatternExternalCall | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |
| TelDisconnectCode | For a description of this parameter, refer to 'Configuring the Voice Mail (VM) Parameters' on page 172. |

6.5.10 PSTN Parameters

Table 6-10: PSTN Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| PCMLawSelect | For a description of this parameter, refer to 'Configuring the TDM Bus Settings' on page 221. |
| ProtocolType | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| ProtocolType_x | Same as the description for parameter ProtocolType, but for a specific trunk ID (x = 0 - 3). |
| TraceLevel | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| FramingMethod | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| FramingMethod_x | Same as the description for parameter FramingMethod, but for a specific trunk ID (x = 0 - 3). |
| TerminationSide | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| TerminationSide_x | Same as the description for parameter TerminationSide, but for a specific trunk ID (x = 0 - 3). |
| ClockMaster | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| ClockMaster_x | Same as the description for parameter ClockMaster, but for a specific trunk ID (x = 0 - 3). |
| TDMBusClockSource | For a description of this parameter, refer to 'Configuring the TDM Bus Settings' on page 221. |
| TDMBusPSTNAutoClock Enable | For a description of this parameter, refer to 'Configuring the TDM Bus Settings' on page 221. |
| TDMBusLocalReference | For a description of this parameter, refer to 'Configuring the TDM Bus Settings' on page 221. |
| AutoClockTrunkPriority | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| TDMBusPSTNAutoClock RevertingEnable | For a description of this parameter, refer to 'Configuring the TDM Bus Settings' on page 221. |
| LineCode | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| LineCode_x | Same as the description for parameter LineCode, but for a specific trunk ID (x = 0 - 3). |
| EnableCallingPartyCategory | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| BChannelNegotiation | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| NFASGroupNumber_x | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| DChConfig_x | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| ISDNNFASInterfaceID_x | For a description of this parameter, refer to 'Trunk Settings' on page 206. |

Table 6-10: PSTN Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| CASTableIndex_x | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| CASFileName_0 CASFileName_1 CASFileName_7 | CAS file name (e.g., 'E_M_WinkTable.dat') that defines the CAS protocol. It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the gateway trunks using the parameter CASTableIndex_x. |
| CASTablesNum | 1 to 8. Indicates how many CAS protocol configurations files are loaded. |
| IdleABCDPattern | For a description of this parameter, refer to 'Configuring the TDM Bus Settings' on page 221. |
| IdlePCMPattern | For a description of this parameter, refer to 'Configuring the TDM Bus Settings' on page 221. |
| LineBuildOut.Loss | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| ISDNRxOverlap_x | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| ISDNRxOverlap | <p>[0] = Disabled (default). [1] = Enabled. Any number bigger than one = Number of digits to receive. Notes:</p> <ul style="list-style-type: none"> ▪ If enabled, the gateway receives ISDN called number that is sent in the 'Overlap' mode. ▪ The INVITE to IP is sent only after the number (including 'Sending Complete' Info Element) was fully received (in SETUP and/or subsequent INFO Q.931 messages). <p>For detailed information on ISDN overlap dialing, refer to ISDN Overlap Dialing on page 444.</p> |
| R2Category | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161 |
| HeldTimeout | <p>Determines the time period the gateway can stay on-hold. If a Resume (un-hold Re- INVITE) message is received before the timer expires, the call is renewed. If this timer expires, the call is released.</p> <ul style="list-style-type: none"> ▪ [-1] = Indefinitely (default). ▪ [0 - 2400] =Time to wait in seconds. <p>Currently applicable only to MFC R2 CAS variants.</p> |
| CallPriorityMode | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| MLPPDefaultNamespace | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| SIPDefaultCallPriority | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| MLPPDiffserv | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |

Table 6-10: PSTN Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| TrunkLifeLineType | Defines the type of trunk lifeline. Short trunks 1-2, 3-4. <ul style="list-style-type: none"> [0] = Activate lifeline on power down (default). [1] = Activate lifeline on power down or on detection of LAN disconnect. [2] = Activate lifeline on power down or on detection of LAN disconnect or loss of ping. |
| TrunkAdministrativeState | Defines the administrative state of a trunk. <ul style="list-style-type: none"> [0] = Lock the trunk; stops trunk traffic to configure the trunk protocol type. [2] = Unlock the trunk (default); enables trunk traffic. |
| ISDN Flexible Behavior Parameters ISDN protocol is implemented in different Switches / PBXs by different vendors. Several implementations vary a little from the specification. Therefore, to provide a flexible interface that supports these ISDN variants, the ISDN behavior parameters are used. | |
| ISDNInCallsBehavior | For a description of this parameter, refer to 'Trunk Settings' on page 206 . |
| ISDNIBehavior | For a description of this parameter, refer to 'Trunk Settings' on page 206 . |
| ISDNGeneralCCBehavior | For a description of this parameter, refer to 'Trunk Settings' on page 206 . |
| ISDNOutCallsBehavior | For a description of this parameter, refer to 'Trunk Settings' on page 206 . |
| ISDNIBehavior_x | Same as the description for parameter ISDNIBehavior, but for a specific trunk ID. |
| ISDNInCallsBehavior_x | Same as the description for parameter ISDNInCallsBehavior, for a specific trunk ID. |
| ISDNOutCallsBehavior_x | Same as the description for parameter ISDNOutCallsBehavior, but for a specific trunk ID. |
| PlayRBTone2Tel | For a description of this parameter, refer to 'General Parameters' on page 72 . |
| PlayRBTone2IP | For a description of this parameter, refer to 'General Parameters' on page 72 . |
| ProgressIndicator2IP | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| SendMetering2IP | This parameter is now obsolete. |
| TimeForReorderTone | For a description of this parameter, refer to Configuring the FXO Parameters on page 168 . |
| DisconnectOnBusyTone | For a description of this parameter, refer to Configuring the FXO Parameters on page 168 . |

Table 6-10: PSTN Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| EnableVoiceDetection | <p>For a description of this parameter, refer to Configuring the FXO Parameters on page 168.</p> <ul style="list-style-type: none"> ▪ [1] = The gateway sends 200 OK (to INVITE) messages when speech/fax/modem is detected. ▪ [0] = The gateway sends 200 OK messages immediately after the gateway finishes dialing (default). <p>Usually this feature is used only when early media is used to establish voice path before the call is answered.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ To activate this feature, set EnableDSIPMDetectors to 1. ▪ This feature is applicable only when the protocol type is CAS. |
| DigitMapping | For a description of this parameter, refer to 'DTMF & Dialing Parameters' on page 98. |
| TimeBetweenDigits | For a description of this parameter, refer to 'DTMF & Dialing Parameters' on page 98. |
| MaxDigits | For a description of this parameter, refer to 'DTMF & Dialing Parameters' on page 98. |
| TimeForDialTone | For a description of this parameter, refer to 'DTMF & Dialing Parameters' on page 98. |
| RegretTime | For a description of this parameter, refer to 'General Parameters' on page 103. |

6.5.11 ISDN and CAS Interworking-Related Parameters

Table 6-11: ISDN and CAS Interworking-Related Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| EnableTDMoverIP | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| EnableISDNTunnelingTel2IP | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| EnableISDNTunnelingIP2Tel | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| ISDNDuplicateQ931BuffMode | <p>Controls the activation / deactivation of delivering raw Q.931 messages.</p> <ul style="list-style-type: none"> ▪ [0] = ISDN messages aren't duplicated (default). ▪ [128] = All ISDN messages are duplicated. <p>Note: This parameter is not updated on-the-fly and requires a gateway reset.</p> |

Table 6-11: ISDN and CAS Interworking-Related Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| EnableQSIGTunneling | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| PlayRBTone2Trunk_ID | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| DefaultCauseMapISDN2IP | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| CauseMapSIP2ISDN | <p>Defines a flexible mapping of SIP Responses and Q.850 Release Causes. Format of this <i>ini</i> file parameter table:</p> <pre>[CauseMapSIP2ISDN] FORMAT CauseMapSIP2ISDN_Index = CauseMapSIP2ISDN_SipResponse, CauseMapSIP2ISDN_IsdnReleaseCause; \[CauseMapSIP2ISDN]</pre> <p>Where,</p> <ul style="list-style-type: none"> SipResponse = SIP Response IsdnReleaseCause = Q.850 Release Cause <p>For example:</p> <pre>[CauseMapSIP2ISDN] CauseMapSIP2ISDN 0 = 480,50; CauseMapSIP2ISDN 0 = 404,3; \[CauseMapSIP2ISDN]</pre> <p>When a SIP response is received (from the IP side), the gateway searches this mapping table for a match. If the SIP response is found, the Release Cause assigned to it is sent to the PSTN. If no match is found, the default static mapping is used.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter can appear up to 12 times. For an explanation on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. |

Table 6-11: ISDN and CAS Interworking-Related Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| CauseMapISDN2SIP | <p>Defines a flexible mapping of Q.850 Release Causes to SIP Responses. Format of this <i>ini</i> file parameter table:</p> <pre>[CauseMapISDN2SIP] FORMAT CauseMapISDN2SIP_Index = CauseMapISDN2SIP_IsdnReleaseCause, CauseMapISDN2SIP_SipResponse; [\\CauseMapISDN2SIP]</pre> <p>Where,</p> <ul style="list-style-type: none"> IsdnReleaseCause = Q.850 Release Cause SipResponse = SIP Response <p>For example:</p> <pre>[CauseMapISDN2SIP] CauseMapISDN2SIP 0 = 50,480; CauseMapISDN2SIP 0 = 6,406; [\\CauseMapISDN2SIP]</pre> <p>When a Release Cause is received (from the PSTN side), the gateway searches this mapping table for a match. If the Q.850 Release Cause is found, the SIP response assigned to it is sent to the IP side. If no match is found, the default static mapping is used.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter can appear up to 12 times. For an explanation on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. |
| SITQ850Cause | <p>Determines the Q.850 cause value specified in the Reason header that is included in a 4xx response when Special Information Tone (SIT) is detected on an IP-to-Tel call.</p> <p>The valid range is 0 to 127. The default value is 34.</p> |
| UserToUserHeaderFormat | <p>Determines the format of the User-to-User header.</p> <ul style="list-style-type: none"> [0] = X-UserToUser (default) [1] = User-to-User |
| RemoveCLIWhenRestricted | <p>For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161.</p> |
| ScreeningInd2ISDN | <p>For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161.</p> |
| ProgressIndicator2ISDN_ID | <p>For a description of this parameter, refer to 'Trunk Settings' on page 206.</p> |
| PIForDisconnectMsg_ID | <p>For a description of this parameter, refer to 'Trunk Settings' on page 206.</p> |

Table 6-11: ISDN and CAS Interworking-Related Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| ConnectOnProgressInd | <ul style="list-style-type: none"> [0] = Connect message isn't sent after 183 Session Progress is received (default). [1] = Connect message is sent after 183 Session Progress is received. <p>This feature enables the play of announcements from IP to PSTN without the need to answer the Tel-to-IP call. It can be used with PSTN networks that don't support the opening of a TDM channel before an ISDN Connect message is received.</p> |
| SIP183Behavior | For a description of this parameter, refer to 'General Parameters' on page 72. |
| LocalISDNRBSource_ID | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| PSTNAlertTimeout | For a description of this parameter, refer to 'General Parameters' on page 103. |
| TrunkPSTNAlertTimeout_ID | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| ISDNTransferCapability_ID | For a description of this parameter, refer to 'Trunk Settings' on page 206. |
| SendISDNTransferOnConnect | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| ISDNSubAddressFormat | <p>Determines the format of the Subaddress value for ISDN Calling and Called numbers.</p> <ul style="list-style-type: none"> [0] = ASCII (default). [1] = BCD. <p>For IP-to-Tel calls, if the incoming INVITE message includes 'Subaddress' values for the Called Number (in the Request-URI) and/or the Calling Number (in the From header), these values are interworked to the outgoing ISDN Setup message.</p> <p>If the incoming ISDN SETUP message includes 'subaddress' values for the Called Number and/or the Calling Number, these values are interworked to the outgoing SIP INVITE message.</p> |
| EnableHold2ISDN | <p>Enables interworking of the Hold/Retrieve supplementary service from SIP to PRI.</p> <ul style="list-style-type: none"> [0] = Disabled (default) [1] = Enabled <p>Notes:</p> <ul style="list-style-type: none"> This capability is supported only for QSIG and Euro ISDN variants. To support interworking of the Hold/Retrieve supplementary service from ISDN to SIP, set EnableHold = 1. |
| EnableUUITel2IP | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| EnableUUUIP2Tel | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |

Table 6-11: ISDN and CAS Interworking-Related Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| ScreeningInd2IP | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| SupportRedirectInFacility | <ul style="list-style-type: none"> ▪ [0] = Not Supported (default). ▪ [1] = Supports partial retrieval of Redirect Number (number only) from a Facility IE in ISDN Setup messages. Applicable to Redirect number according to ECMA-173 Call Diversion Supplementary Services. <p>Note: To enable this feature, 'ISDNDuplicateQ931BuffMode' must be set to 1.</p> |
| EnableCIC | <ul style="list-style-type: none"> ▪ [0] = Do not relay the Carrier Identification Code (CIC) to ISDN (default). ▪ [1] = CIC is relayed to ISDN in Transit Network Selection IE. <p>If enabled, the CIC code (received in an INVITE Request-URI) is included in a TNS IE in ISDN Setup message. For example: INVITE sip:555666;cic=2345@100.2.3.4 sip/2.0. Note: Currently, this feature is supported only in the SIP-to-ISDN direction.</p> |
| EnableAOC | <ul style="list-style-type: none"> ▪ [0] = Not used (default). ▪ [1] = ISDN Advice of Charge (AOC) messages are interworked to SIP. <p>The gateway supports reception of ISDN (Euro ISDN) AOC messages. AOC messages can be received during a call (Facility messages) or at the end of a call (Disconnect or Release messages). The gateway converts the AOC messages into SIP INFO (during a call) and BYE (end of a call) messages using a proprietary AOC SIP header. The gateway supports both Currency and Pulse AOC messages.</p> |
| PlayBusyTone2ISDN | For a description of this parameter, refer to 'General Parameters' on page 72. |

Table 6-11: ISDN and CAS Interworking-Related Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| TrunkTransferMode_X | <ul style="list-style-type: none"> [0] = Not supported (default). [1] = Supports CAS NFA DMS-100 transfer. When a SIP REFER message is received, the gateway performs a Blind Transfer by executing a CAS Wink, waits for an acknowledge Wink from the remote side, dials the Refer-to number to the switch, and then releases the call. Note: A specific NFA CAS table is required. [2] = Supports ISDN transfer: RLT (DMS-100), TBCT (NI2), and ECT (EURO ISDN). When a SIP REFER message is received, the gateway performs a transfer by sending FACILITY messages to the PBX with the necessary information on the call's legs that are to be connected. The different ISDN variants use slightly different methods (using FACILITY messages) to perform the transfer. [3] = Supports CAS Normal transfer. When a SIP REFER message is received, the gateway performs a Blind Transfer by executing a CAS Wink, dialing the Refer-to number to the switch and then releasing the call. [4] = Supports QSIG Single Step transfer. IP-to-Tel: When a SIP REFER message is received, the gateway performs a transfer by sending a FACILITY message to the PBX, initiating Single Step transfer. Once a success return result is received, the transfer is completed. Tel-to-IP: When a FACILITY message initiating Single Step transfer is received from the PBX, a REFER message is sent to the IP side. <p>To configure Trunk Transfer Mode using the Embedded Web Server, refer to 'Trunk Settings' on page 206.</p> |
| CASTransportType | For a description of this parameter, refer to 'Configuring the Voice Settings' on page 191 . |
| CASAddressingDelimiters | <p>Determines if delimiters are added to the dialed address or dialed ANI parameters.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable <p>When this parameter is enabled, delimiters such as '*', '#', and 'ST' are added to the dialed address or dialed ANI parameters. When it is disabled, the address and ANI strings remain without delimiters.</p> |
| CASDelimitersPaddingUsage | <p>Defines the digits string delimiter padding usage per trunk.</p> <ul style="list-style-type: none"> [0] (default) = default address string padding: '*XXX#' (where XXX is the digit string that begins with '*' and ends with '#', when using padding). [1] = special use of asterisks delimiters: '*XXX*YYY*' (where XXX is the address, YYY is the source phone number, and '*' is the only delimiter padding). |
| CasStateMachineGenerateDigitOnTime | For a description of this parameter, refer to 'CAS State Machines' on page 219 . |

Table 6-11: ISDN and CAS Interworking-Related Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|---|
| CasStateMachineGenerateInterDigitTime | For a description of this parameter, refer to 'CAS State Machines' on page 219. |
| CasStateMachineDTMFMaxOnDetectionTime | For a description of this parameter, refer to 'CAS State Machines' on page 219. |
| CasStateMachineDTMFMinOnDetectionTime | For a description of this parameter, refer to 'CAS State Machines' on page 219. |
| CasStateMachineMaxNumOfIncomingAddressDigits | For a description of this parameter, refer to 'CAS State Machines' on page 219. |
| CasStateMachineMaxNumOfIncomingANIDigits | For a description of this parameter, refer to 'CAS State Machines' on page 219. |
| CasStateMachineCollectANI | For a description of this parameter, refer to 'CAS State Machines' on page 219. |
| CasStateMachineDigitSignalingSystem | For a description of this parameter, refer to 'CAS State Machines' on page 219. |
| EnableDSPIPMDetectors | <p>Enables / disables the gateway's DSP detectors.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default). ▪ [1] = Enable. <p>Notes:</p> <ul style="list-style-type: none"> ▪ The gateway's Feature Key should contain the "IPMDetector" DSP option. ▪ When = 1, the number of available gateway channels is reduced. |
| XChannelHeader | For a description of this parameter, refer to General Parameters on page 103. |
| AddIEinSetup | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| SendIEonTG | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| ISDNDMSTimerT310 | <p>Overrides the T310 timer for the DMS-100 ISDN variant. T310 defines the timeout between the reception of Proceeding message and the reception of Alert / Connect message. The valid range is 10 to 30. The default value is 10 (seconds).</p> <p>Note: Applicable only to Nortel DMS and Nortel MERIDIAN PRI variants (ProtocolType = 14 and 35).</p> |
| ISDNJapanNTTTimerT3JA | <p>T3_JA timer (in seconds). This parameter overrides the internal PSTN T301 timeout on the Users Side (TE side). If an outgoing call from the gateway to ISDN is not answered during this timeout, the call is released. The valid range is 10 to 240. The default value is 50. Applicable only to Japan NTT PRI variant (ProtocolType = 16).</p> <p>Note: This timer is also affected by the parameter PSTNAlertTimeout.</p> |

Table 6-11: ISDN and CAS Interworking-Related Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| EnablePatternDetect or | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| PDPattern | Defines the patterns that can be detected by the Pattern Detector. The valid range is 0 to 0xFF. |
| PDThreshold | Defines the number of consecutive patterns to trigger the pattern detection event. The valid range is 0 to 31. The default is 5. |
| EarlyAnswerTimeout | Defines the time (in seconds) the gateway waits for a CONNECT response from the called party (Tel side) after sending a SETUP message. If the timer expires, the call is answered by sending a 200 OK message (IP side). The valid range is 0 to 600. The default value is 0 (disable). |

6.5.12 Analog Telephony Parameters

Table 6-12: Analog Telephony Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| FXONumberOfRings | Defines the number of rings before the FXO module answers a call. The valid range is 0 to 255. The default is 0 seconds. |
| ChargeCode | <p>Configures metering tones (and their time intervals) that the FXS modules generate to the Tel side.</p> <p>Format of the <i>ini</i> file parameter table:</p> <pre>[ChargeCode] FORMAT ChargeCode_Index = ChargeCode_EndTime1, ChargeCode_PulseInterval1, ChargeCode_PulsesOnAnswer1, ChargeCode_EndTime2, ChargeCode_PulseInterval2, ChargeCode_PulsesOnAnswer2, ChargeCode_EndTime3, ChargeCode_PulseInterval3, ChargeCode_PulsesOnAnswer3, ChargeCode_EndTime4, ChargeCode_PulseInterval4, ChargeCode_PulsesOnAnswer4; [ChargeCode]</pre> <p>Where,</p> <ul style="list-style-type: none"> EndTime = Period (1 - 4) end time PulseInterval = Period (1 - 4) pulse interval PulsesOnAnswer = Period (1 - 4) pulses on answer <p>For example:</p> <pre>[ChargeCode] ChargeCode 1 = 7,30,1,14,20,2,20,15,1,0,60,1; ChargeCode 2 = 5,60,1,14,20,1,0,60,1; ChargeCode 3 = 0,60,1; ChargeCode 0 = 6, 3, 1, 12, 2, 1, 18, 5, 2, 0, 2, 1; [ChargeCode]</pre> |

Table 6-12: Analog Telephony Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| | <p>Notes:</p> <ul style="list-style-type: none"> For an explanation on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. The parameter can appear up to 25 times (i.e., up to 25 different metering rules can be defined). To configure the Charge Codes table using the Web interface, refer to Charge Codes Table. |
| TargetOfChannel | <p>Defines telephone numbers that are automatically dialed when a specific port is used. Format of this <i>ini</i> file parameter table: [TargetOfChannel] FORMAT TargetOfChannel_Index = TargetOfChannel_Destination, TargetOfChannel_Type, TargetOfChannel_Port, TargetOfChannel_Module; [TargetOfChannel] Where,</p> <ul style="list-style-type: none"> Destination = Destination phone number Type = following values: [1] = Destination phone number is automatically dialed if phone is offhooked (for FXS modules) or ring signal is applied to port (FXO modules). [0] = automatic dialing is disabled. [2] = enables Hotline -- when a phone is offhooked and no digit is pressed for HotLineToneDuration, the destination phone number is automatically dialed. Port = Port number Module = Module number (0 - 5) <p>For example: [TargetOfChannel] TargetOfChannel 1 = 1001,1,0,1; (Automatic dialing on port 1, module 1) [TargetOfChannel]</p> <p>Notes:</p> <ul style="list-style-type: none"> For an explanation on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. The indexing of this <i>ini</i> file parameter table starts with 1. The numbering of channels starts with 0. Define this parameter for each gateway port that implements Automatic Dialing. To configure the Automatic Dialing Table using the Web interface, refer to 'Automatic Dialing' on page 155. |

Table 6-12: Analog Telephony Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| CallerDisplayInfo | <p>[CallerDisplayInfo] FORMAT CallerDisplayInfo_Index = CallerDisplayInfo_DisplayString, CallerDisplayInfo_IsCidRestricted, CallerDisplayInfo_Port, CallerDisplayInfo_Module; [CallerDisplayInfo]</p> <p>Where,</p> <ul style="list-style-type: none"> DisplayString = Caller ID string IsCidRestricted = Restriction: [0] is not restricted (default); [1] is restricted Port = Port number Module = Module number (0 - 5) <p>For example: [CallerDisplayInfo] CallerDisplayInfo 1 = Susan C.,0,1,0; (Caller ID on port 1 of first module) [CallerDisplayInfo]</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. The indexing of this <i>ini</i> file parameter table starts with 1. The numbering of channels starts with 0. To configure Caller Display Information using the Web interface, refer to 'Caller ID' on page 156. |

Table 6-12: Analog Telephony Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| FwdInfo | <p>Forwards IP-to-Tel calls (using 302 response) based on the gateway's port to which the call is routed (applicable only to FXS).</p> <p>[FwdInfo] FORMAT FwdInfo_Index = FwdInfo_Type, FwdInfo_Destination, FwdInfo_NoReplyTime, FwdInfo_Port, FwdInfo_Module; [FwdInfo] Where,</p> <ul style="list-style-type: none"> ▪ Type = Forward Type (for a list of options, refer to 'Call Forward' on page 157). ▪ Destination = Telephone number or URI (number@IP address) to which the call is forwarded. ▪ NoReplyTime = Timeout (in seconds) for No Reply. If you have set the Forward Type for this port to No Answer [3], enter the number of seconds the gateway waits before forwarding the call to the phone number specified ▪ Port = Port number ▪ Module = Module number (0 - 5) <p>For example: [FwdInfo] FwdInfo 1 = 1,1001,\$\$,2,0; FwdInfo 2 = 1,2003@10.5.1.1,\$\$,2,0; FwdInfo 3 = 3,2005,30,2,0; [FwdInfo]</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For an explanation on ini file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. ▪ The indexing of this <i>ini</i> file parameter table starts with 1. ▪ The numbering of gateway ports starts with 0. ▪ To configure the Call Forward table using the Web interface, refer to 'Call Forward' on page 157. |

Table 6-12: Analog Telephony Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| EnableCallerID | <p>Configures Caller ID permissions. Format for this <i>ini</i> file parameter table: [EnableCallerID] FORMAT EnableCallerID_Index = EnableCallerID_IsEnabled, EnableCallerID_Port, EnableCallerID_Module; [EnableCallerID] Where,</p> <ul style="list-style-type: none"> IsEnabled = Enables [1] or disables [0] (default) Caller ID Port = Port number Module = Module number (0 - 5) <p>For example: [EnableCallerID] EnableCallerID 1 = 1,3,2; EnableCallerID 2 = 0,\$\$, \$\$; [EnableCallerID] Notes:</p> <ul style="list-style-type: none"> For an explanation on ini file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. The indexing of this <i>ini</i> file table parameter starts at 1. The numbering of ports starts with 0. If a port isn't configured, its Caller ID generation / detection are determined according to the global parameter EnableCallerID (described in 'Supplementary Services' on page 113). To configure the Call ID Permissions table using the Web interface, refer to 'Caller ID Permissions' on page 159. |
| EnableDIDWink | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| DelayBeforeDIDWink | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| EnableReversalPolarity | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| EnableCurrentDisconnect | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| TelConnectCode | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| CutThrough | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| FXSOOSBehavior | For a description of this parameter, refer to 'General Parameters' on page 103 . |
| NumberOfWaitingIndications | For a description of this parameter, refer to 'Supplementary Services' on page 113 . |
| TimeBetweenWaitingIndications | For a description of this parameter, refer to 'Supplementary Services' on page 113 . |

Table 6-12: Analog Telephony Parameters

| ini File Field Name Web Parameter Name | Valid Range and Description |
|---|---|
| TimeBeforeWaitingIndication | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| WaitingBeepDuration | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| EnableCallerID | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| CallerIDType | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| EnableMWI | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| MWIAncalogLamp | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| MWIDisplay | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| EnableMWISubscription | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| MWIServerIP | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| SubscribeRetryTime | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| MWIExpirationTime | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| StutterToneDuration | For a description of this parameter, refer to 'Supplementary Services' on page 113. |
| PayPhoneMeteringMode | For a description of this parameter, refer to 'Metering Tones' on page 118. |
| MeteringType | For a description of this parameter, refer to 'Metering Tones' on page 118. |
| KeyCFUnCond | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyCFNoAnswer | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyCFBusy | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyCFBusyOrNoAnswer | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyCFDoNotDisturb | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyCFDeact | For a description of this parameter, refer to 'Keypad Features' on page 120. |

Table 6-12: Analog Telephony Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| KeyCLIR | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyCLIRDeact | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyHotLine | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyHotLineDeact | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyBlindTransfer | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyCallWaitingDeact | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| KeyCallWaiting | For a description of this parameter, refer to 'Keypad Features' on page 120. |
| IsTwoStageDial | For a description of this parameter, refer to 'Configuring the FXO Parameters' on page 168. |
| IsWaitForDialTone | For a description of this parameter, refer to 'Configuring the FXO Parameters' on page 168. |
| FXOBetweenRingTime | For a description of this parameter, refer to 'Configuring the FXO Parameters' on page 168. |
| RingsBeforeCallerID | For a description of this parameter, refer to 'Configuring the FXO Parameters' on page 168. |
| DisconnectOnDialTone | For a description of this parameter, refer to 'Configuring the FXO Parameters' on page 168. |
| GuardTimeBetweenCalls | For a description of this parameter, refer to 'Configuring the FXO Parameters' on page 168. |
| NTTDIDSignallingForm | <p>Determines the type of Direct Inward Dialing (DID) signaling support for NTT (Japan) modem: DTMF- or Frequency Shift Keying (FSK)-based signaling. Gateways can be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX.</p> <ul style="list-style-type: none"> ▪ [0] = FSK-based signaling (default) ▪ [1] = DTMF-based signaling <p>Note: Applicable only to FXS modules.</p> |

Table 6-12: Analog Telephony Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| EnableDID | <p>Enables support for Japan NTT 'Modem' Direct Inward Dialing (DID). FXS modules can be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX (applicable to FXS modules). The DID signal can be sent alone or combined with an NTT Caller ID signal.</p> <p>Format for this <i>ini</i> file parameter table: [EnableDID] FORMAT EnableDID_Index = EnableDID_IsEnable, EnableDID_Port, EnableDID_Module; [EnableDID] Where, IsEnable = Enables [1] or disables [0] (default) Japan NTT Modem DID support. Port = Port number Module = Module number For example: [EnableDID] EnableDID 0 = 1,2,0; [EnableDID]</p> <p>Notes:</p> <ul style="list-style-type: none"> For an explanation on ini file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. Applicable only to FXS modules. |
| EnableCallerIDTypeTwo | <p>Disables the generation of Caller ID type 2 when the phone is offhooked.</p> <ul style="list-style-type: none"> [0] = Caller ID type 2 isn't played. [1] = Caller ID type 2 is played (default). |
| PolarityReversalType | <p>Defines the voltage change slope during polarity reversal or wink.</p> <ul style="list-style-type: none"> [0] = Soft (default). [1] = Hard. <p>Notes:</p> <ul style="list-style-type: none"> Some Caller ID signals use reversal polarity and/or wink signals. In these cases it is recommended to set PolarityReversalType to 1 (Hard). Applicable only to FXS modules. |
| CurrentDisconnectDuration | <p>Duration of the current disconnect pulse (in msec). The default is 900 msec, The range is 200 to 1500 msec. Applicable for both FXS and FXO modules. Note: The FXO modules' detection range is +/-200 msec of the parameter's value plus 100. For example, if CurrentDisconnectDuration = 200, the detection range is 100 to 500 msec.</p> |
| CurrentDisconnectDefaultThreshold | <p>Determines the line voltage threshold which, when reached, is considered a current disconnect detection. The valid range is 0 to 20 Volts. The default value is 4 Volts. Note: Applicable only to FXO modules.</p> |

Table 6-12: Analog Telephony Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| TimeToSampleAnalogLineVoltage | Determines the frequency at which the analog line voltage is sampled (after offhook), for detection of the current disconnect threshold. The valid range is 100 to 2500 msec. The default value is 1000 msec. Note: Applicable only to FXO modules. |
| AnalogCallerIDTimingMode | <ul style="list-style-type: none"> [0] = Caller ID is generated between the first two rings (default). [1] = The gateway attempts to find an optimized timing to generate the Caller ID according to the selected Caller ID type. Notes: <ul style="list-style-type: none"> Applicable only to FXS modules. When used with distinctive ringing, the Caller ID signal doesn't change the distinctive ringing timing. |
| BellcoreCallerIDTypeOneSubStandard | Selects the Bellcore Caller ID sub-standard. <ul style="list-style-type: none"> [0] = Between rings (default). [1] = Not ring related. |
| ETSICallerIDTypeOneSubStandard | Selects the ETSI FSK Caller ID Type 1 sub-standard (FXS only). <ul style="list-style-type: none"> [0] = ETSI between rings (default). [1] = ETSI before ring DT_AS. [2] = ETSI before ring RP_AS. [3] = ETSI before ring LR_DT_AS. [4] = ETSI not ring related DT_AS. [5] = ETSI not ring related RP_AS. [6] = ETSI not ring related LR_DT_AS. |
| ETSIVMWITypeOneStandard | Selects the ETSI Visual Message Waiting Indication (VMWI) Type 1 sub-standard. <ul style="list-style-type: none"> [0] = ETSI VMWI between rings (default) [1] = ETSI VMWI before ring DT_AS [2] = ETSI VMWI before ring RP_AS [3] = ETSI VMWI before ring LR_DT_AS [4] = ETSI VMWI not ring related DT_AS [5] = ETSI VMWI not ring related RP_AS [6] = ETSI VMWI not ring related LR_DT_AS |
| BellcoreVMWITypeOneStandard | Selects the Bellcore VMWI sub-standard. <ul style="list-style-type: none"> [0] = Between rings (default). [1] = Not ring related. |

6.5.13 Number Manipulation and Routing Parameters

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| TrunkGroup | <p>Defines the Trunk Group table. [TrunkGroup] FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum, TrunkGroup_FirstTrunkId, TrunkGroup_LastTrunkId, TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId, TrunkGroup_Module; [TrunkGroup] Where, TrunkGroupNum = Trunk group ID (1 to 99) FirstTrunkId = Starting physical trunk number 0 - 3 FirstBChannel = Starting B-channel (from 1) LastBChannel = Ending B-channel (up to 31) FirstPhoneNumber = Phone number associated with the first channel (optional) ProfileId = Optional Tel Profile ID (1 to 9) applied to the group of channels LastTrunkId = Ending physical trunk number Module = Module number</p> <p>For example: [TrunkGroup] TrunkGroup 1 = 0, 0, 0, 1, 31, 401, 0; (E1 span) TrunkGroup 1 = 0, 0, 0, 1, 31, \$\$, 1; TrunkGroup 2 = 1, 2, 2, 1, 24, 3000; (T1 span) TrunkGroup 1 = 0, 0, 3, *, 1000; (4 E1 spans; all B-channels) TrunkGroup 3 = 2, 0, 3, 1, 20, 101, 1; (4 E1 spans; 20 B-channels; module 1) [TrunkGroup]</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter can appear up to four times per module. ▪ To represent all B-channels, use an asterisk (*). ▪ For a description on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. |
| ChannelList | This parameter is obsolete; use the parameter TrunkGroup instead. |
| DefaultNumber | For a description of this parameter, refer to 'DTMF & Dialing Parameters' on page 98 . |
| ChannelSelectMode | For a description of this parameter, refer to 'General Parameters' on page 72 . |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| TrunkGroupSettings | <p>Defines rules for port allocation for specific Trunk Groups. If no rule exists, the global rule defined by ChannelSelectMode applies.</p> <p>Format for this <i>ini</i> file table parameter:</p> <pre>[TrunkGroupSettings] FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupID, TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode, TrunkGroupSettings_GatewayName; [TrunkGroupSettings]</pre> <p>Where,</p> <ul style="list-style-type: none"> TrunkGroupID = Trunk Group ID number. ChannelSelectMode = Channel select mode for the Trunk Group. Available values are identical to those defined by the ChannelSelectMode parameter. RegistrationMode = Registration mode for the Trunk Group (Per Endpoint [0], Per Gateway [1], or Do Not Register [4]). If not configured [-1], the value of AuthenticationMode is used. GatewayName = 'sipgatewayname' used as a hostname in the From header in INVITE and REGISTER messages. If not configured, the 'sipgatewayname' parameter is used. <p>For example:</p> <pre>[TrunkGroupSettings] TrunkGroupSettings 0 = 9,0,0,\$\$; [TrunkGroupSettings]</pre> <p>For a description on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295.</p> <p>For configuring Trunk group settings using the Embedded Web Server, refer to Configuring Trunk Group Settings on page 152.</p> |
| AddTrunkGroupAsPrefix | For a description of this parameter, refer to 'General Parameters' on page 132. |
| AddPortAsPrefix | For a description of this parameter, refer to 'General Parameters' on page 132. |
| ReplaceEmptyDstWithPortNumber | For a description of this parameter, refer to 'General Parameters' on page 132. |
| CopyDestOnEmptySource | <ul style="list-style-type: none"> [0] = Leave Source Number empty (default). [1] = If the Source Number of an incoming Tel to IP call is empty, the Destination Number is copied to the Source Number. |
| AddNPIandTON2CallingNumber | For a description of this parameter, refer to 'General Parameters' on page 132. |
| AddNPIandTON2CalledNumber | For a description of this parameter, refer to 'General Parameters' on page 132. |
| UseSourceNumberAsDisplayNumber | For a description of this parameter, refer to 'General Parameters' on page 132. |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| UseDisplayNameAsSourceNumber | For a description of this parameter, refer to 'General Parameters' on page 72. |
| AlwaysUseRouteTable | For a description of this parameter, refer to 'Proxy & Registration Parameters' on page 84. |
| Prefix | <p>Configures the Tel to IP Routing table to route incoming Tel calls to IP addresses.</p> <p>Format for this <i>ini</i> file table parameter: [Prefix] FORMAT PREFIX_Index = PREFIX_DestinationPrefix, PREFIX_DestAddress, PREFIX_SourcePrefix, PREFIX_ProfileId, PREFIX_MeteringCode, PREFIX_DestPort; [Prefix]</p> <p>Where,</p> <ul style="list-style-type: none"> DestinationPrefix = Destination phone prefix DestAddress = Destination IP address SourcePrefix = Source phone prefix ProfileID = Profile ID number MeteringCode = Charge code DestPort = Destination port <p>For example: [PREFIX] Prefix 0 = 20,10.2.10.2,202,1 Prefix 1 = 10[340-451]xxx#,10.2.10.6,*,1 Prefix 2 = *,gateway.domain.com,*Prefix 3 = 10, 10.13.83.5, *, 0, 255, 0, 5060;[PREFIX]</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. The phone prefix for destination (DestinationPrefix) and source (SourcePrefix) address can be a single number or a range of numbers. This parameter can appear up to 50 times. Parameters can be skipped by using the dollar sign ('\$'), for example: Prefix = \$\$,10.2.10.2,202,1. The destination IP address (DestAddress) can be either in dotted format notation or a FQDN. This field can also include a selected port to use (DestPort). If an FQDN is used, DNS resolution is performed according to DNSQueryType. The IP address can include wildcards. The 'x' wildcard is used to represent single digits, e.g., 10.8.8.xx represents all addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g., 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255. |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| | <ul style="list-style-type: none"> If the string 'ENUM' is specified for the destination IP address, an ENUM query containing the destination phone number is sent to the DNS server. The ENUM reply includes a SIP URI, used as the Request-URI in the outgoing INVITE and for routing (if Proxy is not used). For detailed information on this feature and for configuring the Tel to IP Routing table using the Embedded Web Server, refer to 'Tel to IP Routing Table' on page 134. For available notations, refer to 'Dialing Plan Notation' on page 128. |
| PSTNPrefix | <p>Configures the routing of IP-to-Tel calls to Trunk groups (also configured in the Embedded Web Server's 'IP to Trunk Group Routing Table' screen -- refer to 'IP to Trunk Group Routing' on page 138). Format of this <i>ini</i> file parameter table: [PSTNPrefix] FORMAT PSTNPrefix_Index = PSTNPrefix_DestPrefix, PSTNPrefix_TrunkGroupID, PSTNPrefix_SourcePrefix, PSTNPrefix_SourceAddress, PSTNPrefix_ProfileID; [PSTNPrefix]</p> <p>Where,</p> <ul style="list-style-type: none"> DestPrefix = Destination number prefix TrunkGroupID = Trunk group ID (1 to 99) SourcePrefix = Source number prefix SourceAddress = Source IP address (obtained from the Contact header in the INVITE message) ProfileID = optional IP Profile ID (1 to 4) that can be applied to each routing rule <p>For example: [PSTNPrefix] PSTNPrefix 0 = 10, 2, *, 10.13.8.9, 1; [PSTNPrefix]</p> <p>Notes:</p> <ul style="list-style-type: none"> To support the In-Call Alternative Routing feature, you can use two entries that support the same call, but assigned with a different Trunk group. The second entry functions as an alternative selection if the first rule fails as a result of one of the release reasons listed in the AltRouteCauseIP2Tel table. Selection of Trunk groups (for IP-to-Tel calls) is according to destination number, source number, and source IP address. The source IP address (SourceAddress) can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 and 10.8.8.99. The source IP address (SourceAddress) can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255. If the source IP address (SourceAddress) includes an FQDN, DNS resolution is performed according to DNSQueryType. |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| | <ul style="list-style-type: none"> This parameter can appear up to 24 times. For available notations that represent multiple numbers, refer to 'Dialing Plan Notation' on page 128. |
| RemovePrefix | For a description of this parameter, refer to 'General Parameters' on page 132. |
| RouteModelIP2Tel | For a description of this parameter, refer to 'IP to Trunk Group Routing' on page 138. |
| RouteModeTel2IP | For a description of this parameter, refer to 'Tel to IP Routing Table' on page 134. |
| SwapRedirectNumber | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| Prefix2RedirectNumber | For a description of this parameter, refer to 'Configuring the Digital Gateway Parameters' on page 161. |
| AddTON2RPI | For a description of this parameter, refer to 'General Parameters' on page 72. |
| NumberMapTel2IP | <p>Manipulates the destination number for Tel-to-IP calls (also configured in the Embedded Web Server's 'Destination Phone Number Manipulation Table for Tel→IP Calls'screen -- refer to 'Configuring the Number Manipulation Tables' on page 125).</p> <p>Format of this <i>ini</i> file parameter table:</p> <pre>[NumberMapTel2Ip] FORMAT NumberMapTel2Ip_Index = NumberMapTel2Ip_DestinationPrefix, NumberMapTel2Ip_SourcePrefix, NumberMapTel2Ip_SourceAddress, NumberMapTel2Ip_NumberType, NumberMapTel2Ip_NumberPlan, NumberMapTel2Ip_RemoveFromLeft, NumberMapTel2Ip_RemoveFromRight, NumberMapTel2Ip_LeaveFromRight, NumberMapTel2Ip_Prefix2Add, NumberMapTel2Ip_Suffix2Add, NumberMapTel2Ip_IsPresentationRestricted; [NumberMapTel2Ip]</pre> <p>Where,</p> <ul style="list-style-type: none"> DestinationPrefix = Destination number prefix SourcePrefix = Source number prefix SourceAddress = N/A NumberType = Number Type used in RPID header NumberPlan = Number Type used in RPID header RemoveFromLeft = Number of stripped digits from the left RemoveFromRight = Number of stripped digits from the right LeaveFromRight = Number of remaining digits from the right Prefix2Add = String to add as prefix Suffix2Add = String to add as suffix |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| | <ul style="list-style-type: none"> IsPresentationRestricted = N/A (set to \$\$) <p>For example: [NumberMapTel2Ip] NumberMapTel2Ip 0 = 01,\$\$,*,0,0,2,\$\$,971,\$\$, NumberMapTel2Ip 1 = 10,10,*,255,255,3,0,5,100,\$\$,255; [NumberMapTel2Ip]</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, and NumberPlan are applied if the called and calling numbers match the DestinationPrefix and SourcePrefix conditions. The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. Parameters can be skipped by using two dollar signs ('\$\$'). Number Plan and Type can optionally be used in Remote Party ID (RPID) header by using the EnableRPIHeader and AddTON2RPI parameters. |
| NumberMapIP2Tel | <p>Manipulates the destination number for IP-to-Tel calls (also configured in the Embedded Web Server's 'Destination Phone Number Manipulation Table for IP→Tel Calls' screen -- refer to 'Configuring the Number Manipulation Tables' on page 125).</p> <p>Format of this <i>ini</i> file parameter table: [NumberMapIp2Tel] FORMAT NumberMapIp2Tel_Index = NumberMapIp2Tel_DestinationPrefix, NumberMapIp2Tel_SourcePrefix, NumberMapIp2Tel_SourceAddress, NumberMapIp2Tel_NumberType, NumberMapIp2Tel_NumberPlan, NumberMapIp2Tel_RemoveFromLeft, NumberMapIp2Tel_RemoveFromRight, NumberMapIp2Tel_LeaveFromRight, NumberMapIp2Tel_Prefix2Add, NumberMapIp2Tel_Suffix2Add, NumberMapIp2Tel_IsPresentationRestricted; [NumberMapIp2Tel]</p> <p>Where,</p> <ul style="list-style-type: none"> DestinationPrefix = Destination number prefix SourcePrefix = Source number prefix SourceAddress = Source IP address (obtained from the Contact header in the INVITE message) NumberType = Q.931 Number Type (TON) NumberPlan = Q.931 Number Plan (NPI) RemoveFromLeft = Number of stripped digits from the left RemoveFromRight = Number of stripped digits from the right |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| | <ul style="list-style-type: none"> LeaveFromRight = Number of remaining digits from the right Prefix2Add = String to add as prefix Suffix2Add = String to add as suffix IsPresentationRestricted = N/A (set to \$\$) <p>For example: [NumberMapIp2Tel] NumberMapIp2Tel 0 = 01,034,10.13.77.8,\$\$,0,\$\$,2,\$\$,667,\$\$; NumberMapIp2Tel 1 = 10,10,1.1.1.1,255,255,3,0,5,100,\$\$,255; [NumberMapIp2Tel]</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, and NumberPlan are applied if the called and calling numbers match the DestinationPrefix, SourcePrefix, and SourceAddress conditions. The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. Parameters can be skipped by using two dollar signs ('\$\$'). The Source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all addresses between 10.8.8.10 and 10.8.8.99. The Source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all the addresses between 10.8.8.0 and 10.8.8.255. |
| SourceNumberMapTel2IP | <p>Manipulates the source phone number for Tel-to-IP calls.(also configured in the Embedded Web Server's Source Phone Number Manipulation Table for Tel→IP Calls' screen -- refer to 'Configuring the Number Manipulation Tables' on page 125).</p> <p>Format of this <i>ini</i> file parameter table: [SourceNumberMapTel2Ip] FORMAT SourceNumberMapTel2Ip_Index = SourceNumberMapTel2Ip_DestinationPrefix, SourceNumberMapTel2Ip_SourcePrefix, SourceNumberMapTel2Ip_SourceAddress, SourceNumberMapTel2Ip_NumberType, SourceNumberMapTel2Ip_NumberPlan, SourceNumberMapTel2Ip_RemoveFromLeft, SourceNumberMapTel2Ip_RemoveFromRight, SourceNumberMapTel2Ip_LeaveFromRight, SourceNumberMapTel2Ip_Prefix2Add, SourceNumberMapTel2Ip_Suffix2Add, SourceNumberMapTel2Ip_IsPresentationRestricted; [SourceNumberMapTel2Ip]</p> <p>Where,</p> |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| | <ul style="list-style-type: none"> DestinationPrefix = Destination number prefix SourcePrefix = Source number prefix SourceAddress = Source IP address (obtained from the Request-URI in the INVITE message) NumberType = Number Type used in RPID header NumberPlan = Number Plan used in RPID header RemoveFromLeft = Number of stripped digits from the left RemoveFromRight = Number of stripped digits from the right LeaveFromRight = Number of remaining digits from the right Prefix2Add = String to add as prefix Suffix2Add = String to add as suffix IsPresentationRestricted = Calling number presentation (0 to allow presentation; 1 to restrict presentation) <p>For example: [SourceNumberMapTel2Ip] SourceNumberMapTel2Ip 0 = 22,03,\$\$,0,0,\$\$,2,\$\$,667,\$\$,0; SourceNumberMapTel2Ip 0 = 10,10,*,255,255,3,0,5,100,\$\$,255; [SourceNumberMapTel2Ip]</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, NumberPlan, and IsPresentationRestricted are applied if the called and calling numbers match the DestinationPrefix and SourcePrefix conditions. The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. Parameters can be skipped by using two dollar signs ('\$\$'). An asterisk (*) represents all IP addresses. IsPresentationRestricted is set to 'Restricted' only if 'Asserted Identity Mode' is set to 'P-Asserted'. Number Plan and Type can optionally be used in Remote Party ID (RPID) header by using the EnableRPIHeader and AddTON2RPI parameters. |
| SourceNumberMapIP2Tel | Manipulates the source number for IP-to-Tel calls (also configured in the Embedded Web Server's 'Source Phone Number Manipulation Table for IP→Tel Calls' screen -- refer to 'Configuring the Number Manipulation Tables' on page 125). Format of this <i>ini</i> file parameter table: [SourceNumberMapIp2Tel] FORMAT SourceNumberMapIp2Tel_Index = SourceNumberMapIp2Tel_DestinationPrefix, SourceNumberMapIp2Tel_SourcePrefix, SourceNumberMapIp2Tel_SourceAddress, SourceNumberMapIp2Tel_NumberType, |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| | <p>SourceNumberMapIp2Tel_NumberPlan, SourceNumberMapIp2Tel_RemoveFromLeft, SourceNumberMapIp2Tel_RemoveFromRight, SourceNumberMapIp2Tel_LeaveFromRight, SourceNumberMapIp2Tel_Prefix2Add, SourceNumberMapIp2Tel_Suffix2Add, SourceNumberMapIp2Tel_IsPresentationRestricted; [SourceNumberMapIp2Tel]</p> <p>Where,</p> <ul style="list-style-type: none"> DestinationPrefix = Destination number prefix SourcePrefix = Source number prefix SourceAddress = Source IP address (obtained from the Request-URI in the INVITE message) NumberType = Q.931 Number Type (TON) NumberPlan = Q.931 Number Plan (NPI) RemoveFromLeft = Number of stripped digits from the left RemoveFromRight = Number of stripped digits from the right LeaveFromRight = Number of remaining digits from the right Prefix2Add = String to add as prefix Suffix2Add = String to add as suffix IsPresentationRestricted = Calling number presentation (0 to allow presentation; 1 to restrict presentation) <p>For example: [SourceNumberMapIp2Tel] SourceNumberMapIp2Tel 0 = 22,03,\$,\$,\$,\$,\$,\$,2,667,\$,\$,\$;SourceNumberMapIp2Tel 1 = 034,01,1.1.1.1,\$,\$,0,2,\$,\$,\$,972,\$,\$,10; [SourceNumberMapIp2Tel]</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, and NumberPlan are applied if the called and calling numbers match the DestinationPrefix, SourcePrefix, and SourceAddress conditions. The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. Parameters can be skipped by using two dollar signs ('\$'). The Source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all addresses between 10.8.8.10 and 10.8.8.99. The Source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|---|--|
| | represents all the addresses between 10.8.8.0 and 10.8.8.255. |
| <p>For ETSI ISDN variant, the following Number Plan and Type combinations (Plan/Type) are supported in the Destination and Source Manipulation tables:</p> <ul style="list-style-type: none"> 0,0 = Unknown, Unknown 9,0 = Private, Unknown 9,1 = Private, Level 2 Regional 9,2 = Private, Level 1 Regional 9,3 = Private, PISN Specific 9,4 = Private, Level 0 Regional (local) 1,0 = Public(ISDN/E.164), Unknown 1,1 = Public(ISDN/E.164), International 1,2 = Public(ISDN/E.164), National 1,3 = Public(ISDN/E.164), Network Specific 1,4 = Public(ISDN/E.164), Subscriber 1,6 = Public(ISDN/E.164), Abbreviated <p>For NI-2 and DMS-100 ISDN variants the valid combinations of TON and NPI for calling and called numbers are (Plan/Type):</p> <ul style="list-style-type: none"> 0/0 - Unknown/Unknown 1/1 - International number in ISDN/Telephony numbering plan 1/2 - National number in ISDN/Telephony numbering plan 1/4 - Subscriber (local) number in ISDN/Telephony numbering plan 9/4 - Subscriber (local) number in Private numbering plan | |
| SecureCallsFromIP | For a description of this parameter, refer to 'General Parameters' on page 103 . |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| AltRouteCauseTel2IP | <p>Table of SIP call failure reason values received from the IP side. If a call is released as a result of one of these reasons, the gateway tries to find an alternative route to that call in the 'Tel to IP Routing' table (if Proxy is not used) or used as a redundant Proxy (when Proxy is used).</p> <p>Format for this <i>ini</i> file parameter table: [AltRouteCauseTel2IP] FORMAT AltRouteCauseTel2IP_Index = AltRouteCauseTel2IP_ReleaseCause; [AltRouteCauseTel2IP]</p> <p>For example: [AltRouteCauseTel2IP] AltRouteCauseTel2IP 0 = 486; (Busy here) AltRouteCauseTel2IP 1 = 480; (Temporarily unavailable) AltRouteCauseTel2IP 2 = 408; (No response) [AltRouteCauseTel2IP]</p> <p>Notes:</p> <ul style="list-style-type: none"> For an explanation on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. The 408 reason can be used to specify no response from the remote party to the INVITE request. This parameter can appear up to 5 times. For defining the Reasons for Alternative Routing table using the Embedded Web Server, refer to 'Reasons for Alternative Routing' on page 142. |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| AltRouteCauseIP2Tel | <p>Table of call failure reason values received from the PSTN side (in Q.931 presentation). If a call is released as a result of one of these reasons, the gateway attempts to find an alternative trunk group for that call in the 'IP to Trunk Group Routing' table.</p> <p>Format for this <i>ini</i> file parameter table: [AltRouteCauseIP2Tel] FORMAT AltRouteCauseIP2Tel_Index = AltRouteCauseIP2Tel_ReleaseCause; [AltRouteCauseIP2Tel]</p> <p>For example: [AltRouteCauseIP2Tel] AltRouteCauseIP2Tel 0 = 3 (No route to destination) AltRouteCauseIP2Tel 1 = 1 (Unallocated number) AltRouteCauseIP2Tel 2 = 17 (Busy here) [AltRouteCauseIP2Tel]</p> <p>Notes:</p> <ul style="list-style-type: none"> For an explanation on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. This parameter can appear up to 5 times. If the gateway fails to establish a call to the PSTN because it has no available channels in a specific trunk group (e.g., all trunk group's channels are occupied, or the trunk group's spans are disconnected or out of sync), it uses the Internal Release Cause '3' (no route to destination). This cause can be used in the AltRouteCauseIP2Tel table to define routing to an alternative trunk group. For defining the Reasons for Alternative Routing table using the Embedded Web Server, refer to 'Reasons for Alternative Routing' on page 142. |
| EnableETSIDiversion | <p>Defines the method in which the Redirect Number is passed towards the Tel side.</p> <p>Valid options include:</p> <ul style="list-style-type: none"> [0] = Q.931 Redirecting Number Information Element (default) [1] = ETSI DivertingLegInformation2 in a Facility Information Element |
| FilterCalls2IP | <p>For a description of this parameter, refer to 'General Parameters' on page 103.</p> |
| Alternative Routing Parameters | |
| RedundantRoutingMode | <p>Determines the type of redundant routing mechanism to implement when a call can't be completed using the main route.</p> <ul style="list-style-type: none"> [0] = No redundant routing is used. If the call can't be completed using the main route (either using the active Proxy or the first matching rule in the internal routing table), the call is disconnected. [1] = Internal routing table is used to find a redundant route (default). [2] = Proxy list is used to find a redundant route. |

Table 6-13: Number Manipulation and Routing Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| AltRoutingTel2IPEnable | For a description of this parameter, refer to 'General Parameters' on page 132. |
| AltRoutingTel2IPMode | For a description of this parameter, refer to 'General Parameters' on page 132. |
| IPConnQoSMaxAllowedPL | For a description of this parameter, refer to 'General Parameters' on page 132. |
| IPConnQoSMaxAllowedDelay | For a description of this parameter, refer to 'General Parameters' on page 132. |
| Phone-Context Parameters | |
| AddPhoneContextAsPrefix | For a description of this parameter, refer to 'Mapping NPI/TON to Phone-Context' on page 130. |
| PhoneContext | <p>Defines the Phone Context table. Format for this <i>ini</i> file parameter table: [PhoneContext] FORMAT PhoneContext_Index = PhoneContext_Npi, PhoneContext_Ton, PhoneContext_Context; [PhoneContext] Where,</p> <ul style="list-style-type: none"> ▪ Npi = Number Plan ▪ Ton = Number Type ▪ Context = Phone-Context value <p>When a call is received from the ISDN/Tel, the NPI and TON are compared against the table, and the Phone-Context value is used in the outgoing SIP INVITE message. The same mapping occurs when an INVITE with a Phone-Context attribute is received. The Phone-Context parameter appears in the standard SIP headers where a phone number is used (Request-URI, To, From, Diversion). For example: [PhoneContext] PhoneContext 0 = 0,0,unknown.com PhoneContext 1 = 1,1,host.com PhoneContext 2 = 9,1,na.e164.host.com [PhoneContext]</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For an explanation on <i>ini</i> file parameter tables, refer to 'Structure of ini File Parameter Tables' on page 295. ▪ This parameter can appear up to 20 times. ▪ Several entries with the same NPI-TON or Phone-Context are allowed. In this scenario, a Tel-to-IP call uses the first match. ▪ Phone-Context '+' is a unique as it doesn't appear in the Request-URI as a Phone-Context parameter. Instead, it's added as a prefix to the phone number. The '+' isn't removed from the phone number in the IP-to-Tel direction. ▪ To configure Phone Context table using the Embedded Web Server, refer to 'Mapping NPI/TON to Phone-Context' on page 130. |

6.5.14 Channel Parameters

The Channel Parameters define the DTMF, fax and modem transfer modes.

Table 6-14: Channel Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| DJBufMinDelay | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| DJBufOptFactor | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| AnalogSignalTransportType | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| FaxTransportMode | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| FaxRelayEnhancedRedundancyDepth | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| FaxRelayRedundancyDepth | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| FaxRelayMaxRate | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| FaxRelayECMEnable | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| FaxModemBypassCoderType | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| CNGDetectorMode | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| FaxModemBypassM | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| FaxBypassPayloadType | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| CallerIDTransportType | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| ModemBypassPayloadType | Modem Bypass dynamic payload type (range 0-127). The default value is 103. |
| FaxModemRelayVolume | -18 to -3, corresponding to -18 dBm to -3 dBm in 1 dB steps. The default is -12 dBm fax gain control. |
| DetFaxOnAnswerTone | For a description of this parameter, refer to 'General Parameters' on page 72. |
| EchoCancellerAggressiveNLP | Enables or disables the Aggressive NLP at the first 0.5 second of the call. When enabled, the echo is removed only in the first half a second of the incoming IP signal. <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable |

Table 6-14: Channel Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| FaxModemBypassBasicRTTPa cketInterval | <p>Determines the basic frame size that is used during fax / modem bypass sessions.</p> <ul style="list-style-type: none"> ▪ [0] = Determined internally (default) ▪ [1] = 5 msec (not recommended) ▪ [2] = 10 msec ▪ [3] = 20 msec <p>Note: When set for 5 msec (1), the maximum number of simultaneous channels supported is 120.</p> |
| FaxModemBypassDJBufMinDe lay | <p>Determines the Jitter Buffer delay during fax and modem bypass session. The range is 0 to 150 msec. The default is 40.</p> |
| EnableFaxModemInbandNetw orkDetection | <p>Enables or disables inband network detection related to fax/modem.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>When this parameter is enabled on Bypass mode (VxxTransportType = 2), a detection of an Answer Tone from the network triggers a switch to bypass mode in addition to the local Fax/Modem tone detections. However, only a high bit-rate coder voice session effectively detects the Answer Tone sent by a remote Endpoint. This can be useful when, for example, the payload of voice and bypass is the same, allowing the originator to switch to bypass mode as well.</p> |

Table 6-14: Channel Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| NSEMode | <p>Cisco compatible fax and modem bypass mode.</p> <ul style="list-style-type: none"> [0] = NSE disabled (default) [1] = NSE enabled <p>Notes:</p> <ul style="list-style-type: none"> This feature can be used only if VxxModemTransportType = 2 (Bypass). If NSE mode is enabled, the SDP contains the following line: 'a=rtpmap:100 X-NSE/8000'. To use this feature: <ul style="list-style-type: none"> -- The Cisco gateway must include the following definition: 'modem passthrough nse payload-type 100 codec g711alaw'. -- Set the Modem transport type to Bypass mode (VxxModemTransportType = 2) for all modems. -- Configure the gateway parameter NSEPayloadType = 100. <p>In NSE bypass mode, the gateway starts using G.711 A-Law (default) or G.711μ-Law, according to the parameter FaxModemBypassCoderType. The payload type used with these G.711 coders is a standard one (8 for G.711 A-Law and 0 for G.711 μ-Law). The parameters defining payload type for the 'old' AudioCodes' Bypass mode FaxBypassPayloadType and ModemBypassPayloadType are not used with NSE Bypass. The bypass packet interval is selected according to the parameter FaxModemBypassBasicRtpPacketInterval.</p> |
| NSEPayloadType | <p>NSE payload type for Cisco Bypass compatible mode. The valid range is 96-127. The default value is 105.</p> <p>Note: Cisco gateways usually use NSE payload type of 100.</p> |
| V21ModemTransportType | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| V22ModemTransportType | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| V23ModemTransportType | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| V32ModemTransportType | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| V34ModemTransportType | For a description of this parameter, refer to 'Configuring the Fax / Modem / CID Settings' on page 194. |
| BellModemTransportType | <p>Determines the Bell modem transport method.</p> <ul style="list-style-type: none"> [0] = Transparent (default). [2] = Bypass. [3] = Transparent with events. |
| InputGain | For a description of this parameter, refer to 'Configuring the Voice Settings' on page 191. |

Table 6-14: Channel Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| VoiceVolume | For a description of this parameter, refer to 'Configuring the Voice Settings' on page 191. |
| RTPRedundancyDepth | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| RFC2198PayloadType | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| EnableSilenceCompression | For a description of this parameter, refer to 'Configuring the Voice Settings' on page 191. |
| IsCiscoSCEMode | <ul style="list-style-type: none"> ▪ [0] = No Cisco gateway exists at the remote side (default). ▪ [1] = A Cisco gateway exists at the remote side. <p>When there is a Cisco gateway at the remote side, the local gateway must set the value of the 'annexb' parameter of the fmp attribute in the SDP to 'no'. This logic is used if EnableSilenceCompression = 2 (enable without adaptation). In this case, Silence Suppression is used on the channel, but not declared in the SDP.</p> <p>Note: The IsCiscoSCEMode parameter is only relevant when the selected coder is G.729.</p> |
| EnableEchoCanceller | For a description of this parameter, refer to 'Configuring the Voice Settings' on page 191. |
| MaxEchoCancellerLength | For a description of this parameter, refer to Configuring the General Media Settings on page 205. |
| EchoCancellerAggressiveNLP | <p>Enables or disables the Aggressive Non-Linear Processor (NLP) in the first 0.5 second of the call.</p> <ul style="list-style-type: none"> ▪ [0] = Disabled (default) ▪ [1] = Enabled |
| EnableNoiseReduction | <p>Enables / disables the DSP Noise Reduction mechanism.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default). ▪ [1] = Enable. <p>Note: When this parameter is enabled the channel capacity might be reduced.</p> |
| TestMode | <ul style="list-style-type: none"> ▪ [0] = CoderLoopback, encoder-decoder loopback inside DSP. ▪ [1] = PCMLoopback, loopback the incoming PCM to the outgoing PCM. ▪ [2] = ToneInjection, generates a 1000 Hz tone to outgoing PCM. ▪ [3] = NoLoopback, (default). |
| EnableStandardSIDPayloadType | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |
| ComfortNoiseNegotiation | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198. |

Table 6-14: Channel Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|--|
| RTPSIDCoeffNum | Determines the number of spectral coefficients added to an SID packet being sent according to RFC 3389. Valid only if EnableStandardSIDPayloadType is set to 1. The valid values are [0] (default), [4] , [6] , [8] and [10] . |
| DTMFVolume | For a description of this parameter, refer to 'Configuring the Voice Settings' on page 191. |
| DTMFGenerationTwist | For a description of this parameter, refer to 'Configuring the Voice Settings' on page 191. |
| DTMFInterDigitInterval | Time in msec between generated DTMF digits to PSTN side (if TxDTMFOption = 1, 2 or 3). The default value is 100 msec. The valid range is 0 to 32767. |
| DTMFDigitLength | Time in msec for generating DTMF tones to the PSTN side (if TxDTMFOption = 1, 2 or 3). The default value is 100 msec. The valid range is 0 to 32767. |
| RxDTMFHangOverTime | Defines the Voice Silence time (in msec units) after playing DTMF or MF digits to the Tel / PSTN side that arrive as Relay from the IP side. Valid range is 0 to 2,000 msec. The default is 1,000 msec. |
| TxDTMFHangOverTime | Defines the Voice Silence time (in msec units) after detecting the end of DTMF or MF digits at the Tel / PSTN side when the DTMF Transport Type is either Relay or Mute. Valid range is 0 to 2,000 msec. The default is 100 msec. |
| DTMFTransportType | For a description of this parameter, refer to 'Configuring the Voice Settings' on page 191. |
| AnswerDetectorSensitivity | For a description of this parameter, refer to Configuring the Voice Settings on page 191. |
| RFC2833PayloadType | For a description of this parameter, refer to 'DTMF & Dialing Parameters' on page 98. |
| UDTDetectorFrequencyDeviation | Defines the deviation (in Hz) allowed for the detection of each signal frequency. Units are in Hertz. The valid range is 1 to 50. The default value is 50 Hz. |
| CPTDetectorFrequencyDeviation | Defines the deviation (in Hz) allowed for the detection of each CPT signal frequency. The valid range is 1 to 30. The default value is 10 Hz. |
| MGCPDTMFDetectionPoint | <ul style="list-style-type: none"> [0] = DTMF event is reported on the end of a detected DTMF digit. [1] = DTMF event is reported on the start of a detected DTMF digit (default). |
| MinFlashHookTime | For a description of this parameter, refer to 'Configuring the Hook-Flash Settings' on page 204. |
| FlashHookOption | For a description of this parameter, refer to 'DTMF & Dialing Parameters' on page 98. |
| FlashHookPeriod | For a description of this parameter, refer to 'Configuring the Hook-Flash Settings' on page 204. |

Table 6-14: Channel Parameters

| <i>ini</i> File Field Name Web Parameter Name | Valid Range and Description |
|--|---|
| AnalogSignalTransportType | This parameter is obsolete; use instead the parameter HookFlashOption. |
| VQMonEnable | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198 . |
| RTCPInterval | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198 . |
| DisableRTCPRandomize | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198 . |
| RTCPXREscIP | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198 . |
| RTCPXRReportMode | For a description of this parameter, refer to 'Configuring the RTP / RTCP Settings' on page 198 . |

6.5.15 Configuration Files Parameters

The configuration files (i.e., auxiliary files) can be loaded to the gateway using the Embedded Web Server or a TFTP session (refer to 'Auxiliary Files' on page 269). Before you load them to the gateway, in the *ini* file you need to specify the files that you want loaded and whether they must be stored in the non-volatile memory. The table below lists the *ini* file parameters associated with these configuration files:

Table 6-15: Configuration Files Parameters

| <i>ini</i> File Field Name | Valid Range and Description |
|---------------------------------------|--|
| CallProgressTonesFilename | The name of the file containing the Call Progress Tones definitions. Refer to the <i>SIP Series Reference Manual</i> for additional information on how to create and load this file. |
| FXSLoopCharacteristicsFileName | The name (and path) of the file providing the FXS line characteristic parameters. |
| FXOLoopCharacteristicsFileName | The name (and path) of the file providing the FXO line characteristic parameters. |
| CASFileName | This is the name of the file containing specific CAS protocol definition (such as 'E_M_WinkTable.dat'). These files are provided to support various types of CAS signaling. |
| CASFileName_x | CAS file name (e.g., 'E_M_WinkTable.dat') that defines the CAS protocol. It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the gateway trunks using the parameter CASTableIndex_x. |
| CASTablesNum | Number, 1 to 8. Specifies how many CAS configuration files are loaded. |
| VoicePromptsFileName | The name (and path) of the file containing the Voice Prompts definitions. Refer to the <i>SIP Series Reference Manual</i> for additional information on how to create and load this file. |
| PrerecordedTonesFileName | The name (and path) of the file containing the Prerecorded Tones. |
| CasTrunkDialPlanName | The Dial Plan name (up to 11-character strings) that is used on the specific trunk. |
| DialPlanFileName | The name (and path) of the file containing dial-plan configuration for CAS and SIP protocols. This file should be constructed using the TrunkPack Conversion Utility (refer to the <i>SIP Series Reference Manual</i>) supplied as part of the software package on the CD accompanying the gateway. |
| UserInfoFileName | The name (and path) of the file containing the User Information data. |
| SaveConfiguration | Determines if the gateway's configuration (parameters and files) is saved to flash (non-volatile memory). <ul style="list-style-type: none"> [0] = Configuration isn't saved to flash memory. [1] = Configuration is saved to flash memory (default). |

7 Telephony Capabilities

This section describes the gateway's telephony capabilities.

7.1 Configuring the DTMF Transport Types

You can control the way DTMF digits are transported over the IP network to the remote endpoint. The following five modes are supported:

- Using INFO message according to the Nortel IETF draft:
In this mode DTMF digits are carried to the remote side within INFO messages.
To enable this mode, define the following:

- RxDTMFOption = 0 (**Protocol Management** menu > **Protocol Definition** submenu > **DTMF & Dialing** option > 'Declare RFC 2833 in SDP' = No)
- TxDTMFOption = 1 (1st to 5th DTMF Option = INFO (Nortel))

Note that in this mode, DTMF digits are erased from the audio stream [DTMFTransportType is automatically set to 0 (DTMF Mute)].

- Using INFO message according to Cisco's mode:
In this mode, DTMF digits are carried to the remote side within INFO messages.
To enable this mode, define the following:

- RxDTMFOption = 0 (Declare RFC 2833 in SDP = No)
- TxDTMFOption = 3 (1st to 5th DTMF Option = INFO (Cisco))

Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0 (DTMF Mute)).

- Using NOTIFY messages according to <draft-mahy-sipping-signaled-digits-01.txt>:
In this mode, DTMF digits are carried to the remote side using NOTIFY messages.
To enable this mode, define the following:

- RxDTMFOption = 0 (Declare RFC 2833 in SDP = No)
- TxDTMFOption = 2 (1st to 5th DTMF Option = NOTIFY)

Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0 (DTMF Mute)).

- Using RFC 2833 relay with Payload type negotiation:
In this mode, DTMF digits are carried to the remote side as part of the RTP stream in accordance with RFC 2833 standard.
To enable this mode, define the following:

- TxDTMFOption = 4 (1st to 5th DTMF Option = RFC 2833)
- RxDTMFOption = 3 (Declare RFC 2833 in SDP = Yes)

Note that to set the RFC 2833 payload type with a different value (other than its default, 96) configure the RFC2833PayloadType (RFC 2833 Payload Type) parameter. The gateway negotiates the RFC 2833 payload type using local and remote SDP and sends packets using the PT from the received SDP. The gateway expects to receive RFC 2833 packets with the same PT as configured by the RFC2833PayloadType parameter. If the remote side doesn't include 'telephony-event' in its SDP, the gateway sends DTMF digits in transparent mode (as part of the voice stream).

- Sending DTMF digits (in RTP packets) as part of the audio stream (DTMF Relay is disabled):
Note that this method is normally used with G.711 coders; with other low-bit rate (LBR) coders the quality of the DTMF digits is reduced.
To enable this mode, define the following:

- TxDTMFOption = 0 (1st to 5th DTMF Option = Disable)
- RxDTMFOption = 0 (Declare RFC 2833 in SDP = No)
- DTMFTransportType = 2 (DTMF Transport Type = Transparent DTMF)

- Using INFO message according to Korea mode:
In this mode, DTMF digits are carried to the remote side within INFO messages.
To enable this mode, define the following:

- RxDTMFOption = 0 (Declare RFC 2833 in SDP = No)
- TxDTMFOption = 3 (1st to 5th DTMF Option = INFO (Korea))

Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0 (DTMF Mute)).



Notes:

- The gateway is always ready to receive DTMF packets over IP, in all possible transport modes: INFO messages, NOTIFY, and RFC 2833 (in proper payload type) or as part of the audio stream.
- To exclude RFC 2833 Telephony event parameter from the gateway's SDP, set RxDTMFOption to 0 in the *ini* file.

The following parameters affect the way the SIP gateway handles the DTMF digits:

- TxDTMFOption, RxDTMFOption, and RFC2833PayloadType (described in 'DTMF & Dialing Parameters' on page 98)
- MGCPDTMFDetectionPoint, DTMFVolume, DTMFTransportType, DTMFDigitLength, and DTMFInterDigitInterval (refer to 'Channel Parameters' on page 372)

7.2 Fax and Modem Capabilities

7.2.1 Fax/Modem Operating Modes

The gateway supports two modes of operations:

- Fax / modem negotiation isn't performed during the establishment of the call.
- VBD mode for V.152 implementation (refer to 'Supporting V.152 Implementation' on page 387): in this mode, fax / modem capabilities are negotiated between the gateway and the remote endpoint at the establishment of the call. During a call, when a fax / modem signal is detected, change from voice to VBD (or T.38) is automatically performed and no additional SIP signaling is required. If negotiation fails (i.e., no match is achieved for any of the transport capabilities), fallback to existing logic occurs (according to the parameter IsFaxUsed).

7.2.2 Fax/Modem Transport Modes

The gateway supports the following transport modes for fax and each modem type (V.22/V.23/Bell/V.32/V.34):

- T.38 fax relay (refer to 'Fax Relay Mode' on page 381)
- Fax and modem bypass: a proprietary method that uses a high bit rate coder (refer to 'Fax/Modem Bypass Mode' on page 382)
- NSE Cisco's Pass-through bypass mode for fax and modem (refer to 'Fax / Modem NSE Mode' on page 383)
- Transparent: passing the fax / modem signal in the current voice coder (refer to 'Fax / Modem Transparent Mode' on page 385)
- Transparent with events: passing the fax / modem signal in the current voice coder with adaptations (refer to 'Fax / Modem Transparent with Events Mode' on page 385)
- G.711 Transport: switching to G.711 when fax/modem is detected (refer to 'G.711 Fax / Modem Transport Mode' on page 384)
- Fax fallback to G.711 if T.38 is not supported (refer to 'Fax Fallback' on page 384)

'Adaptations' refer to automatic reconfiguration of certain DSP features to treat fax/modem streams differently than voice.

7.2.2.1 T.38 Fax Relay Mode

In this mode, fax signals are transferred using T.38 protocol. T.38 is an ITU standard for sending fax across IP networks in a real-time mode. The gateway currently supports only the T.38 UDP syntax.

T.38 can be configured in the following two ways:

- Switching to T.38 mode using SIP Re-INVITE messages (refer to 'Switching to T.38 Mode using SIP Re-INVITE' on page 381)
- Automatically switching to T.38 mode without using SIP Re-INVITE messages (refer to 'Automatically Switching to T.38 Mode without SIP Re-INVITE' on page 382)

When fax transmission has ended, the reverse switching from fax relay to voice is automatically performed at both the local and remote endpoints.

You can change the fax rate that is declared in the SDP using the parameter FaxRelayMaxRate (this parameter doesn't affect the actual transmission rate) and can enable/disable Error Correction Mode (ECM) fax mode using the FaxRelayECMEnable parameter.

When using T.38 mode, you can define a redundancy feature to improve fax transmission over congested IP networks. This feature is activated using the FaxRelayRedundancyDepth and FaxRelayEnhancedRedundancyDepth parameters. Although this is a proprietary redundancy scheme, it should not create problems when working with other T.38 decoders.

7.2.2.1.1 Switching to T.38 Mode using SIP Re-INVITE

In this mode, the terminating gateway on detection of a fax signal, negotiates T.38 capabilities using a Re-INVITE message. If the far-end gateway doesn't support T.38, the fax fails.

In this mode, the parameter FaxTransportMode is ignored.

To configure T.38 mode using SIP Re-INVITE messages, set IsFaxUsed to 1. Additional configuration parameters include the following:

- FaxRelayEnhancedRedundancyDepth
- FaxRelayRedundancyDepth
- FaxRelayECMEnable
- FaxRelayMaxRate

7.2.2.1.2 Automatically Switching to T.38 Mode without SIP Re-INVITE

In this mode, when a fax signal is detected the channel automatically switches from the current voice coder to answer tone mode, and then to T.38-compliant fax relay mode.

To configure automatic T.38 mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 1
- Additional configuration parameters:
 - FaxRelayEnhancedRedundancyDepth
 - FaxRelayRedundancyDepth
 - FaxRelayECMEnable
 - FaxRelayMaxRate

7.2.2.2 Fax/Modem Bypass Mode

In this proprietary mode, when fax or modem signals are detected, the channel automatically switches from the current voice coder to a high bit-rate coder (according to the parameter FaxModemBypassCoderType). In addition, the channel is automatically reconfigured with the following fax / modem adaptations: switches off silence suppression, enables echo cancellation for fax and disables it for modem, and performs certain jitter buffering optimizations. The network packets generated and received during the bypass period are regular voice RTP packets (per the selected bypass coder), but with a different RTP payload type (according to the parameters FaxBypassPayloadType and ModemBypassPayloadType).

During the bypass period, the coder uses the packing factor, which is defined by the parameter FaxModemBypassM. The packing factor determines the number of coder payloads (each the size of FaxModemBypassBasicRTPPacketInterval) that are used to generate a single fax/modem bypass packet.

When fax/modem transmission ends, the reverse switching, from bypass coder to regular voice coder, is carried out.

To configure fax / modem bypass mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 2
- V21ModemTransportType = 2
- V22ModemTransportType = 2
- V23ModemTransportType = 2

- V32ModemTransportType = 2
- V34ModemTransportType = 2
- BellModemTransportType = 2
- Additional configuration parameters:
 - FaxModemBypassCoderType
 - FaxBypassPayloadType
 - ModemBypassPayloadType
 - FaxModemBypassBasicRTTPacketInterval
 - FaxModemBypassDJBufMinDelay



Notes: When the gateway is configured for modem bypass and T.38 fax, V.21 low-speed modems are not supported and fail as a result.

7.2.2.3 Fax / Modem NSE Mode

In this mode, fax and modem signals are transferred using Cisco-compatible Pass-through bypass mode. On detection of fax or modem answering tone signal, the terminating gateway sends three to six special NSE RTP packets (using NSEpayloadType, usually 100). These packets signal the remote gateway to switch to G.711 coder (according to the parameter FaxModemBypassCoderType). After a few NSE packets are exchanged between the gateways, both gateways start using G.711 packets with standard payload type (8 for G.711 A-Law and 0 for G.711 Mu-Law). In this mode, no Re-INVITE messages are sent. The voice channel is optimized for fax/modem transmission (same as for usual bypass mode).

The parameters defining payload type for the proprietary AudioCodes' Bypass mode FaxBypassPayloadType and ModemBypassPayloadType are not used with NSE Bypass.

When configured for NSE mode, the gateway includes in its SDP the following line:

```
a=rtpmap:100 X-NSE/8000
```

(where 100 is the NSE payload type)

The Cisco gateway must include the following definition: "modem passthrough nse payload-type 100 codec g711alaw".

To configure NSE mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 2
- NSEMode = 1
- NSEPayloadType = 100
- V21ModemTransportType = 2
- V22ModemTransportType = 2
- V23ModemTransportType = 2
- V32ModemTransportType = 2

- V34ModemTransportType = 2
- BellModemTransportType = 2

7.2.2.4 G.711 Fax / Modem Transport Mode

In this mode, when the terminating gateway detects fax or modem signals (CED or AnsAM), it sends a Re-INVITE message to the originator gateway asking it to reopen the channel in G.711 VBD with the following adaptations:

- Echo Canceller = off
- Silence Compression = off
- Echo Canceller Non-Linear Processor Mode = off
- Dynamic Jitter Buffer Minimum Delay = 40
- Dynamic Jitter Buffer Optimization Factor = 13

After a few seconds upon detection of fax V.21 preamble or super G3 fax signals, the gateway sends a second Re-INVITE enabling the echo canceller (the echo canceller is disabled only on modem transmission).

A 'gpmd' attribute is added to the SDP according to the following format:

- **For G.711A-law:** a=gpmd:0 vbd=yes;ecan=on (or off, for modems)
- **For G.711 μ -law:** a=gpmd:8 vbd=yes;ecan=on (or off for modems)

The parameters FaxTransportMode and VxxModemTransportType are ignored and are automatically set to the mode called 'transparent with events'.

To configure fax / modem transparent mode, set IsFaxUsed to 2.

7.2.2.5 Fax Fallback

In this mode, when the terminating gateway detects a fax signal, it sends a Re-INVITE message to the originator gateway with T.38. If the remote gateway doesn't support T.38 (replies with 415 Media Not Supported), the gateway sends a new Re-INVITE with G.711 VBD with the following adaptations:

- Echo Canceller = on
- Silence Compression = off
- Echo Canceller Non-Linear Processor Mode = off
- Dynamic Jitter Buffer Minimum Delay = 40
- Dynamic Jitter Buffer Optimization Factor = 13

When the gateway initiates a fax session using G.711, a 'gpmd' attribute is added to the SDP according to the following format:

- **For G.711A-law:** a=gpmd:0 vbd=yes;ecan=on
- **For G.711 μ -law:** a=gpmd:8 vbd=yes;ecan=on

In this mode, the parameter FaxTransportMode is ignored and automatically set to 'transparent'.

To configure fax fallback mode, set IsFaxUsed to 3.

7.2.2.6 Fax / Modem Transparent Mode

In this mode, fax and modem signals are transferred using the current voice coder without notifications to the user and without automatic adaptations. It's possible to use the Profiles mechanism (refer to 'Configuring the Profile Definitions' on page 144) to apply certain adaptations to the channel that is used for fax / modem. For example, to use the coder G.711, to set the jitter buffer optimization factor to 13, and to enable echo cancellation for fax and disable it for modem.

To configure fax / modem transparent mode:

- IsFaxUsed = 0
- FaxTransportMode = 0
- V21ModemTransportType = 0
- V22ModemTransportType = 0
- V23ModemTransportType = 0
- V32ModemTransportType = 0
- V34ModemTransportType = 0
- BellModemTransportType = 0
- Additional configuration parameters:
 - CoderName
 - DJBufOptFactor
 - SCE
 - ECE

7.2.2.7 Fax / Modem Transparent with Events Mode

In this mode, fax and modem signals are transferred using the current voice coder with the following automatic adaptations:

- Echo Canceller = on (or off, for modems)
- Echo Canceller Non-Linear Processor Mode = off
- Jitter buffering optimizations

To configure fax / modem transparent with events mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 3
- V21ModemTransportType = 3
- V22ModemTransportType = 3
- V23ModemTransportType = 3
- V32ModemTransportType = 3
- V34ModemTransportType = 3
- BellModemTransportType = 3

7.2.3 Supporting V.34 Faxes

Unlike T.30 fax machines, V.34 fax machines have no relay standard to transmit the data over IP to the remote side. Therefore, the gateway provides the following operation modes for transporting V.34 fax data over the IP:

- Using bypass mechanism for V.34 fax transmission (refer to 'Using Bypass Mechanism for V.34 Fax Transmission' on page 386)
- Using relay mode, i.e., fallback to T.38 (refer to 'Using Relay mode for both T.30 and V.34 faxes' on page 386)



Note: The CNG detector is disabled (CNGDetectorMode = 0) in all the following examples.

7.2.3.1 Using Bypass Mechanism for V.34 Fax Transmission

In this proprietary scenario, the gateway uses bypass (or NSE) mode to transmit V.34 faxes, enabling the full utilization of its speed.

Configure the following parameters to use bypass mode for both T.30 and V.34 faxes:

- FaxTransportMode = 2 (Bypass)
- V34ModemTransportType = 2 (Modem bypass)
- V32ModemTransportType = 2
- V23ModemTransportType = 2
- V22ModemTransportType = 2

Configure the following parameters to use bypass mode for V.34 faxes and T.38 for T.30 faxes:

- FaxTransportMode = 1 (Relay)
- V34ModemTransportType = 2 (Modem bypass)
- V32ModemTransportType = 2
- V23ModemTransportType = 2
- V22ModemTransportType = 2

7.2.3.2 Using Relay mode for both T.30 and V.34 faxes

In this scenario, V.34 fax machines are forced to use their backward compatibility with T.30 faxes and operate in the slower T.30 mode.

Use the following parameters to use T.38 mode for both V.34 faxes and T.30 faxes:

- FaxTransportMode = 1 (Relay)
- V34ModemTransportType = 0 (Transparent)
- V32ModemTransportType = 0

- V23ModemTransportType = 0
- V22ModemTransportType = 0

7.2.4 Supporting V.152 Implementation

The gateway supports the ITU-T recommendation V.152 (Procedures for Supporting Voice-Band Data over IP Networks). Voice-band data (VBD) is the transport of modem, facsimile, and text telephony signals over a voice channel of a packet network with a codec appropriate for such signals.

For V.152 capability, the gateway supports T.38 as well as VBD codecs (i.e., G.711 A-law and G.711 μ -law). The selection of capabilities is performed using the coders table.

When in VBD mode for V.152 implementation, support is negotiated between the gateway and the remote endpoint at the establishment of the call. During this time, initial exchange of call capabilities is exchanged in the outgoing SDP. These capabilities include whether VBD is supported and associated RTP payload types ('gpmd' SDP attribute), supported codecs, and packetization periods for all codec payload types ('ptime' SDP attribute). After this initial negotiation, no Re-INVITE messages are necessary as both endpoints are synchronized in terms of the other side's capabilities. If negotiation fails (i.e., no match was achieved for any of the transport capabilities), fallback to existing logic occurs (according to the parameter IsFaxUsed).

Below is an example of media descriptions of an SDP indicating support for V.152.

```
v=0
o=- 0 0 IN IPV4 <IPAddressA>
s=-
t=0 0
p=+1
c=IN IP4 <IPAddressA>
m=audio <udpPort A> RTP/AVP 18 0
a=ptime:10
a=rtpmap:96 PCMU/8000
a=gpmd: 96 vbd=yes
```

In the example above, V.152 implementation is supported (using the dynamic payload type 96 and G.711 u-law as the VBD codec) as well as the voice codecs G.711 μ -law and G.729.

Instead of using VBD transport mode, the V.152 implementation can use alternative relay fax transport methods (e.g., fax relay over IP using T.38). The preferred V.152 transport method is indicated by the SDP 'pmft' attribute. Omission of this attribute in the SDP content means that VBD mode is the preferred transport mechanism for voice-band data.

To configure T.38 mode use the CoderName parameter.

7.3 FXO Operating Modes

This section provides a description of the FXO operating modes and gateway configurations for Tel-to-IP and IP-to-Tel calls.

7.3.1 IP-to-Telephone Calls

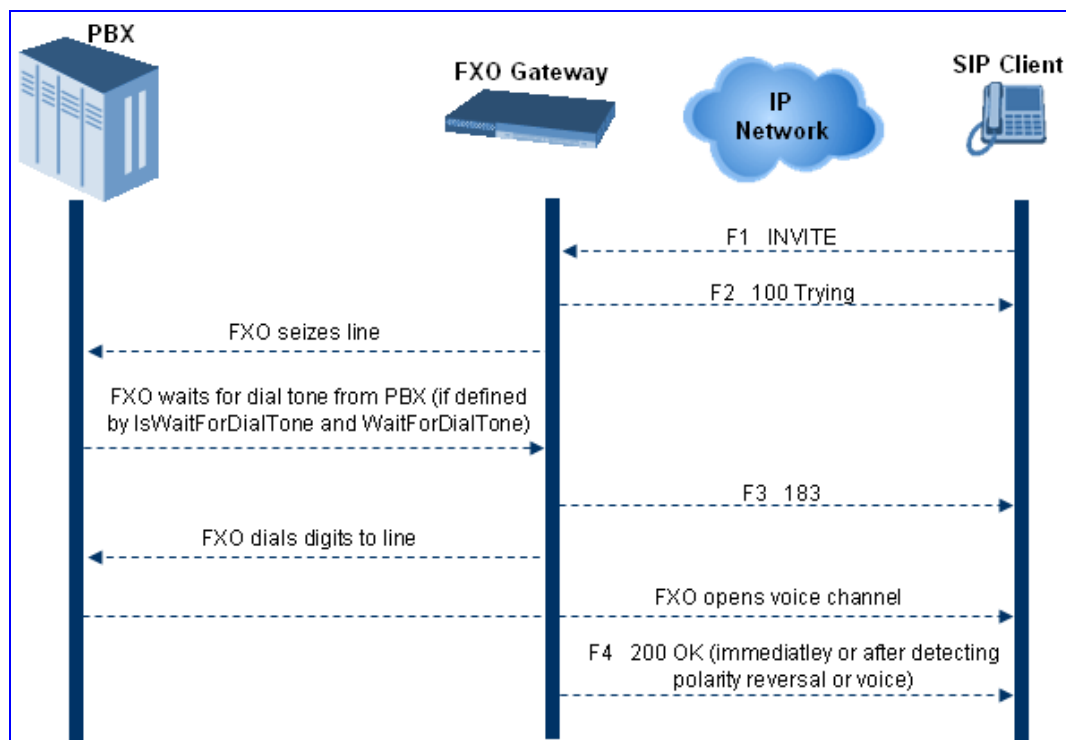
The FXO gateway provides the following operating modes for IP-to-Tel calls:

- One-stage dialing
 - Waiting for dial tone
 - Time to wait before dialing
 - Answer supervision
- Two-stage dialing
- Dialing time
 - Disconnect supervision
 - DID wink

7.3.1.1 One-Stage Dialing

One-stage dialing is when the FXO gateway receives an IP-to-Tel call, off-hooks the PBX line connected to the telephone, and then immediately dials the destination telephone number. In other words, the IP caller doesn't dial the PSTN number upon hearing a dial tone.

Figure 7-1: Call Flow for One-Stage Dialing



One -stage dialing incorporates the following FXO functionality:

■ **Waiting for Dial Tone**

The Waiting for Dial Tone feature enables the gateway to dial the digits to the Tel side only after detecting a dial tone from the PBX line. The *ini* file parameter `IsWaitForDialTone` is used to configure this operation.

■ **Time to Wait Before Dialing**

The Time to Wait Before Waiting feature defines the time (in msec) between seizing the FXO line and starting to dial the digits. The *ini* file parameter `WaitForDialTime` is used to configure this operation.



Note: The *ini* file parameter `IsWaitForDialTone` must be disabled for this mode.

■ **Answer Supervision**

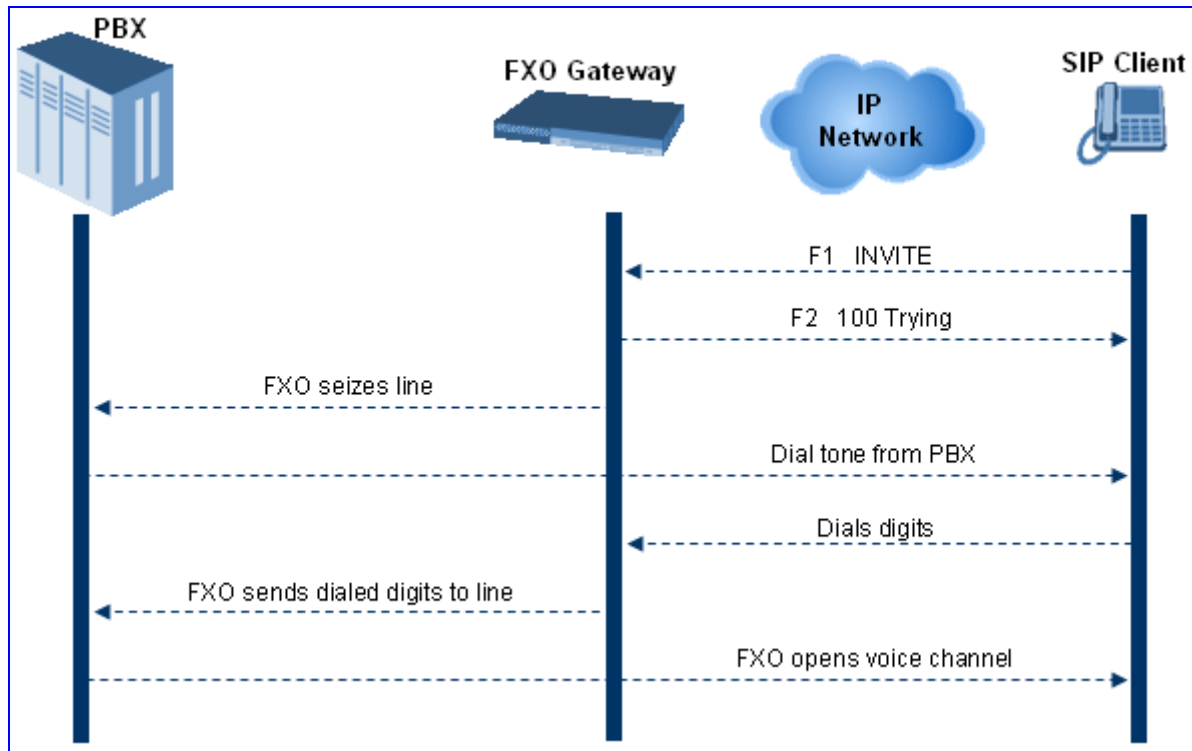
The Answer Supervision feature enables the FXO gateway to determine when a call is connected, by using one of the following methods:

- Polarity Reversal: the gateway sends a 200 OK in response to an INVITE only when it detects a polarity reversal.
- Voice Detection: the gateway sends a 200 OK in response to an INVITE only when it detects the start of speech (or ringback tone) from the Tel side. (Note that the IPM detectors must be enabled).

7.3.1.2 Two-Stage Dialing

Two-stage dialing is when the IP caller is required to dial twice. The caller initially dials to the FXO gateway and only after receiving a dial tone from the PBX (via the FXO gateway) dials the destination telephone number.

Figure 7-2: Call Flow for Two-Stage Dialing



Two-stage dialing implements the Dialing Time feature. Dialing Time allows you to define the time that each digit can be separately dialed. By default, the overall dialing time per digit is 200 msec. The longer the telephone number, the greater the dialing time will be.

The relevant parameters for configuring Dialing Time include the following:

- DTMFDigitLength (100 msec): time for generating DTMF tones to the PSTN (PBX) side
- DTMFInterDigitInterval (100 msec): time between generated DTMF digits to PSTN (PBX) side

7.3.1.3 Call Termination (Disconnect Supervision) on Mediant 1000/FXO

The FXO Disconnect Supervision enables the gateway's FXO ports to monitor call-progress tones from a PBX or from the PSTN. This allows the FXO to determine when the call has terminated on the PBX side, and thereby, prevents analog trunks (i.e., lines to the PBX) from getting "stuck" when the called phone hangs up.

The PBX doesn't disconnect the call, but instead signals to the gateway that the call is disconnected using one of the following methods:

- **Detection of polarity reversal / current disconnect:**

The call is immediately disconnected after polarity reversal or current disconnect is detected on the Tel side (assuming the PBX / CO produces this signal). This is the recommended method.

Relevant parameters: EnableReversalPolarity, EnableCurrentDisconnect, CurrentDisconnectDuration, CurrentDisconnectDefaultThreshold, and TimeToSampleAnalogLineVoltage.

- **Detection of Reorder, Busy, Dial, and Special Information Tone (SIT) tones:**

The call is immediately disconnected after a Reorder, Busy, Dial, or SIT tone is detected on the Tel side (assuming the PBX / CO generates this tone). This method requires the correct tone frequencies and cadence to be defined in the Call Progress Tones file. If these frequencies are not known, define them in the CPT file (the tone produced by the PBX / CO must be recorded and its frequencies analyzed -- refer to Adding a Reorder Tone to the CPT File in the Reference Manual). This method is slightly less reliable than the previous one. You can use the CPTWizard (described in Call Progress Tones Wizard in the Reference Manual) to analyze Call Progress Tones generated by any PBX or telephone network.

Relevant parameters: DisconnectOnBusyTone and DisconnectOnDialTone.

- **Detection of silence:**

The call is disconnected after silence is detected on both call directions for a specific (configurable) amount of time. The call isn't disconnected immediately; therefore, this method should only be used as a backup option.

Relevant parameters: EnableSilenceDisconnect and FarEndDisconnectSilencePeriod.

- **Special DTMF code:**

A digit pattern that when received from the Tel side, indicates to the gateway to disconnect the call.

Relevant *ini* file parameter: TelDisconnectCode.

- **Interruption of RTP stream:**

Relevant parameters: BrokenConnectionEventTimeout and DisconnectOnBrokenConnection.



Note: This method operates correctly only if silence suppression is not used.

- **Protocol-based termination of the call from the IP side**



Note: The implemented disconnect method must be supported by the CO or PBX.

7.3.1.4 DID Wink

The gateway's FXO ports support Direct Inward Dialing (DID). DID is a service offered by telephone companies that enables callers to dial directly to an extension on a PBX without the assistance of an operator or automated call attendant. This service makes use of DID trunks, which forward only the last three to five digits of a phone number to the PBX. If, for example, a company has a PBX with extensions 555-1000 to 555-1999, and a caller dials 555-1234, the local central office (CO) would forward, for example, only 234 to the PBX. The PBX would then ring extension 234.

DID wink enables the originating end to seize the line by going off-hook. It waits for acknowledgement from the other end before sending digits. This serves as an integrity check that identifies a malfunctioning trunk and allows the network to send a re-order tone to the calling party.

The "start dial" signal is a wink from the PBX to the FXO gateway. The FXO then sends the last four to five DTMF digits of the called number. The PBX uses these digits to complete the routing directly to an internal station (telephone or equivalent)

- DID Wink can be used for connection to EIA/TIA-464B DID Loop Start lines
- Both FXO (detection) and FXS (generation) are supported

7.3.2 Telephone-to-IP Calls

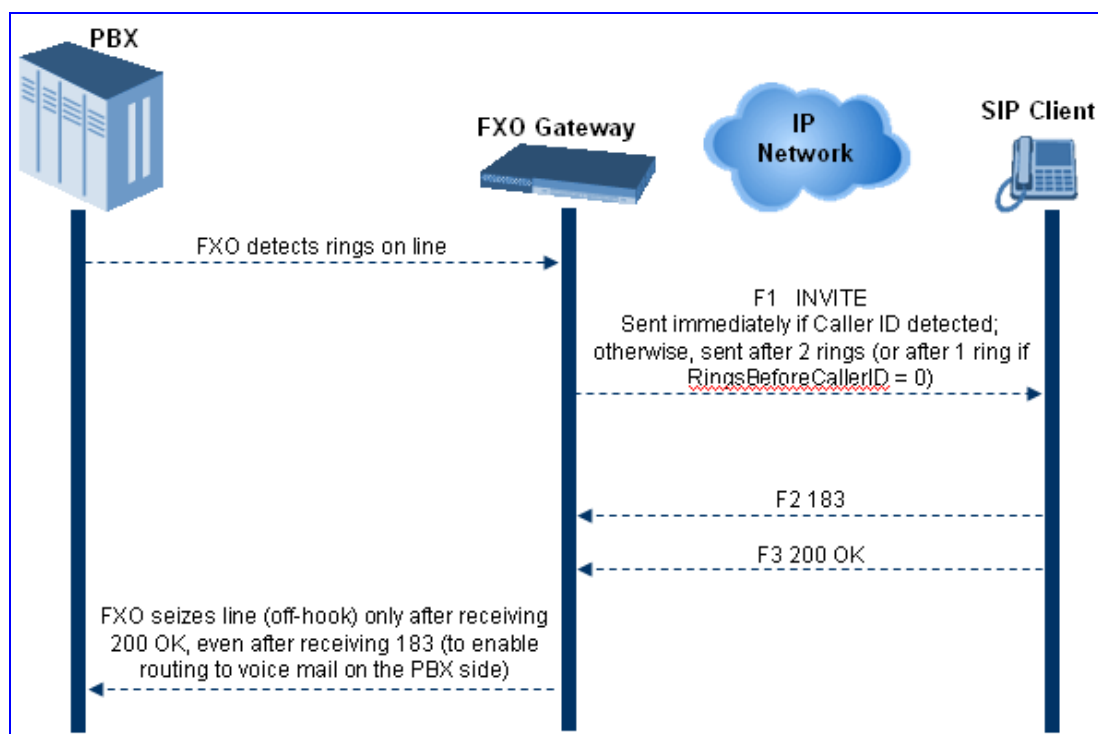
The FXO gateway provides the following FXO operating modes for Tel-to-IP calls:

- Automatic Dialing
- Collecting Digits Mode
- Ring Detection Timeout
- FXO Supplementary Services
 - Hold/Transfer Toward the Tel side
 - Hold/Transfer Toward the IP side
 - Blind Transfer to the Tel side

7.3.2.1 Automatic Dialing

Automatic dialing is defined using the *ini* file parameter table TargetOfChannel (refer to 'Analog Telephony Parameters' on page 350) or the embedded Web server's 'Automatic Dialing' screen (refer to 'Automatic Dialing' on page 155).

The SIP call flow diagram below illustrates Automatic Dialing.

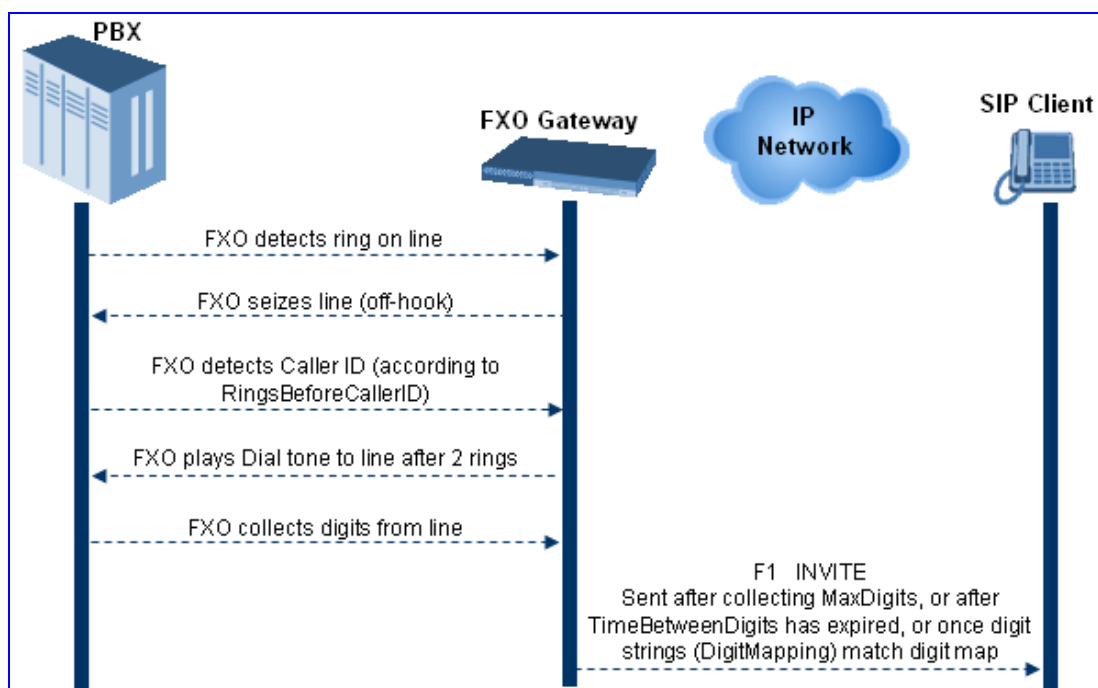


7.3.2.2 Collecting Digits Mode

When automatic dialing is not defined, the gateway collects the digits.

The SIP call flow diagram below illustrates the Collecting Digits Mode.

Figure 7-3: Call Flow for Collecting Digits Mode



7.3.2.3 Ring Detection Timeout

The *ini* file parameters `IsWaitForDialTone` and `WaitForDialTone` apply to Ring Detection Timeout. The operation of Ring Detection Timeout depends on the following:

- No automatic dialing and Caller ID is enabled: if the second ring signal doesn't arrive for Ring Detection Timeout, the gateway doesn't initiate a call to the IP.
- Automatic dialing is enabled: if the remote party doesn't answer the call, and the ringing signal stops for Ring Detection Timeout, the FXO releases the IP call.

Ring Detection Timeout supports full ring cycle of ring on and ring off (from ring start to ring start).

7.3.2.4 FXO Supplementary Services

■ Hold / Transfer toward the Tel side

The *ini* file parameter `LineTransferMode` must be set to 0 (default).

If the FXO receives a hook-flash from the IP side (using out-of-band or RFC 2833), the gateway sends the hook-flash to the Tel side by one of the following:

- Performing a hook flash (i.e., on-hook and off-hook)
- Sending a hook-flash code (defined by the *ini* file parameter `HookFlashCode`)

The PBX may generate a dial tone that is sent to the IP, and the IP side may dial digits of a new destination.

■ Blind Transfer to the Tel side

A blind transfer is one in which the transferring phone connects the caller to a destination line before ringback begins. The *ini* file parameter `LineTransferMode` must be set to 1.

The blind transfer call process is as follows:

- FXO receives a REFER request from the IP side
- FXO sends a hook-flash to the PBX, dials the digits (that are received in the Refer-To header), and then drops the line (on-hook). Note that the time between flash to dial is according to the `WaitForDialTime` parameter.
- PBX performs the transfer internally

■ Hold / Transfer toward the IP side

The FXO gateway doesn't initiate hold / transfer as a response to input from the Tel side. If the FXO receives a REFER request (with or without replaces), it generates a new INVITE according to the Refer-To header.

7.4 Event Notification using X-Detect Header

The gateway supports the sending of notifications to a remote party notifying the occurrence (or detection) of certain events on the media stream. Event detection and notifications is performed using the X-Detect SIP message header, and only when establishing a SIP dialog.

For supporting some events, certain gateway configurations need to be performed. The table below lists the support event types (and subtypes) and the corresponding gateway configurations, if required:

Table 7-1: Supported X-Detect Event Types

| Events | | Required Configuration |
|--------|-------------|--|
| Type | Subtype | |
| CPT | SIT | SITDetectorEnable = 1 UserDefinedToneDetectorEnable = 1 Note: Differentiation of SIT is not supported in 5.0. |
| FAX | CED | (IsFaxUsed ≠ 0) or (IsFaxUsed = 0, and FaxTransportMode ≠ 0) |
| | modem | VxxModemTransportType = 3 |
| PTT | voice-start | EnableDSPIPMDetectors = 1 |
| | voice-end | |

The X-Detect event notification process is as follows:

1. For IP-to-Tel or Tel-to-IP calls, the gateway receives a SIP request message (using the X-Detect header) that the remote party wishes to detect events on the media stream. For incoming (IP-to-Tel) calls, the request must be indicated in the initial INVITE and responded to either in the 183 response (for early dialogs) or in the 200 OK response (for confirmed dialogs). For outgoing calls (Tel-to-IP), the request may be received in the 183 (for early dialogs) and responded to in the PRACK, or received in the 200 OK (for confirmed dialogs) and responded to in the ACK.
2. Once the gateway receives such a request, it sends a SIP response message (using the X-Detect header) to the remote party, listing all supported events that can be detected. The absence of the X-Detect header indicates that no detections are available.
3. Each time the gateway detects a supported event, the event is notified to the remote party, by sending an INFO message with the following message body:
 - Content-Type: application/X-DETECT
 - Type = [CPT | FAX | PTT...]
 - Subtype = xxx (according to the defined subtypes of each type)

Below is an example of SIP messages implementing the X-Detect header:

```

INVITE sip:101@10.33.2.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
Max-Forwards: 70
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:100@10.33.2.53>
X-Detect: Request=CPT,FAX
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>;tag=1c19282
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:101@10.33.2.53>
X-Detect: Response=CPT,FAX
INFO sip:101@10.33.2.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
Max-Forwards: 70
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:100@10.33.2.53>
X-Detect: Response=CPT,FAX
Content-Type: Application/X-Detect
Content-Length: xxx
Type = CPT
Subtype = SIT

```

7.5 RTP Multiplexing (ThroughPacket)

The gateway supports a proprietary method to aggregate RTP streams from several channels to reduce the bandwidth overhead caused by the attached Ethernet, IP, UDP, and RTP headers, and to reduce the packet / data transmission rate. This option reduces the load on network routers and can typically save 50% (e.g., for G.723) on IP bandwidth. RTP Multiplexing (ThroughPacket™) is accomplished by aggregating payloads from several channels that are sent to the same destination IP address into a single IP packet.

RTP multiplexing can be applied to the entire gateway (refer to 'Configuring the RTP / RTCP Settings' on page 198) or to specific IP destinations using the IP Profile feature (refer to 'IP Profile Settings' on page 148).

To enable RTP Multiplexing, set the parameter RemoteBaseUDPPort to a nonzero value. Note that the value of RemoteBaseUDPPort on the local gateway must equal the value of BaseUDPPort of the remote gateway. The gateway uses these parameters to identify and distribute the payloads from the received multiplexed IP packet to the relevant channels.

In RTP Multiplexing mode, the gateway uses a single UDP port for all incoming multiplexed packets and a different port for outgoing packets. These ports are configured using the parameters L1L1ComplexTxUDPPort and L1L1ComplexRxUDPPort.

When RTP Multiplexing is used, call statistics aren't available (since there is no RTCP flow).



Notes:

- RTP Multiplexing must be enabled on both gateways.
- When VLANs are implemented, the RTP Multiplexing mechanism is not supported.

7.6 Dynamic Jitter Buffer Operation

Voice frames are transmitted at a fixed rate. If the frames arrive at the other end at the same rate, voice quality is perceived as good. In many cases, however, some frames can arrive slightly faster or slower than the other frames. This is called jitter (delay variation), and degrades the perceived voice quality. To minimize this problem, the gateway uses a jitter buffer. The jitter buffer collects voice packets, stores them and sends them to the voice processor in evenly spaced intervals.

The gateway uses a dynamic jitter buffer that can be configured using the following two parameters:

- **Minimum delay:** DJBufMinDelay (0 msec to 150 msec)
Defines the starting jitter capacity of the buffer. For example, at 0 msec, there is no buffering at the start. At the default level of 10 msec, the gateway always buffers incoming packets by at least 10 msec worth of voice frames.
- **Optimization Factor:** DJBufOptFactor (0 to 12, 13)
Defines how the jitter buffer tracks to changing network conditions. When set at its maximum value of 12, the dynamic buffer aggressively tracks changes in delay (based on packet loss statistics) to increase the size of the buffer and doesn't decay back down. This results in the best packet error performance, but at the cost of extra delay. At the minimum value of 0, the buffer tracks delays only to compensate for clock drift and quickly decays back to the minimum level. This optimizes the delay performance but at the expense of a higher error rate.

The default settings of 10 msec Minimum delay and 10 Optimization Factor should provide a good compromise between delay and error rate. The jitter buffer 'holds' incoming packets for 10 msec before making them available for decoding into voice. The coder polls frames from the buffer at regular intervals in order to produce continuous speech. As long as delays in the network do not change (jitter) by more than 10 msec from one packet to the next, there is always a sample in the buffer for the coder to use. If there is more than 10 msec of delay at any time during the call, the packet arrives too late. The coder tries to access a frame and is not able to find one. The coder must produce a voice sample even if a frame is not available. It therefore compensates for the missing packet by adding a Bad-Frame-Interpolation (BFI) packet. This loss is then flagged as the buffer being too small. The dynamic algorithm then causes the size of the buffer to increase for the next voice session. The size of the buffer may decrease again if the gateway notices that the buffer is not filling up as much as expected. At no time does the buffer decrease to less than the minimum size configured by the Minimum delay parameter.

For certain scenarios, the **Optimization Factor is set to 13**: One of the purposes of the Jitter Buffer mechanism is to compensate for clock drift. If the two sides of the VoIP call are not synchronized to the same clock source, one RTP source generates packets at a lower rate, causing under-runs at the remote Jitter Buffer. In normal operation (optimization factor 0 to 12), the Jitter Buffer mechanism detects and compensates for the clock drift by occasionally dropping a voice packet or by adding a BFI packet.

Fax and modem devices are sensitive to small packet losses or to added BFI packets. Therefore, to achieve better performance during modem and fax calls, the Optimization Factor should be set to 13. In this special mode the clock drift correction is performed less frequently - only when the Jitter Buffer is completely empty or completely full. When such condition occurs, the correction is performed by dropping several voice packets simultaneously or by adding several BFI packets simultaneously, so that the Jitter Buffer returns to its normal condition.

7.7 Configuring Alternative Routing (Based on Connectivity and QoS)

The Alternative Routing feature enables reliable routing of Tel-to-IP calls when a Proxy isn't used. The gateway periodically checks the availability of connectivity and suitable Quality of Service (QoS) before routing. If the expected quality cannot be achieved, an alternative IP route for the prefix (phone number) is selected.



Note: If the alternative routing destination is the gateway itself, the call can be configured to be routed back to one of the gateway's trunk groups and thus, back into the PSTN (PSTN Fallback).

7.7.1 Alternative Routing Mechanism

When a Tel→IP call is routed through the gateway, the call's destination number is compared to the list of prefixes defined in the Tel to IP Routing table (described in 'Tel to IP Routing Table' on page 134). The Tel to IP Routing table is scanned for the destination number's prefix starting at the top of the table. When an appropriate entry (destination number matches one of the prefixes) is found; the prefix's corresponding destination IP address is checked. If the destination IP address is disallowed, an alternative route is searched for in the following table entries.

Destination IP address is disallowed if no ping to the destination is available (ping is continuously initiated every seven seconds), when an inappropriate level of QoS was detected, or when DNS host name is not resolved. The QoS level is calculated according to delay or packet loss of previously ended calls. If no call statistics are received for two minutes, the QoS information is reset.

The gateway matches the rules starting at the top of the table. For this reason, enter the main IP route above any alternative route.

7.7.2 Determining the Availability of Destination IP Addresses

To determine the availability of each destination IP address (or host name) in the routing table, one (or all) of the following (configurable) methods are applied:

- **Connectivity:** The destination IP address is queried periodically (currently only by ping).
- **QoS:** The QoS of an IP connection is determined according to RTCP statistics of previous calls. Network delay (in msec) and network packet loss (in percentage) are separately quantified and compared to a certain (configurable) threshold. If the calculated amounts (of delay or packet loss) exceed these thresholds, the IP connection is disallowed.
- **DNS resolution:** When host name is used (instead of IP address) for the destination route, it is resolved to an IP address by a DNS server. Connectivity and QoS are then applied to the resolved IP address.

7.7.3 PSTN Fallback as a Special Case of Alternative Routing

The PSTN Fallback feature enables the gateway to redirect PSTN originated calls back to the legacy PSTN network if a destination IP route is unsuitable (disallowed) for voice traffic at a specific time.

To enable PSTN fallback, assign the IP address of the gateway as an alternative route to the desired prefixes. Note that calls (now referred to as IP-to-Tel calls) can be re-routed to a specific trunk group using the Routing parameters (refer to 'IP to Trunk Group Routing' on page 138).

7.7.4 Relevant Parameters

The following parameters (described in 'General Parameters' on page 132) are used to configure the Alternative Routing mechanism:

- AltRoutingTel2IPEnable
- AltRoutingTel2IPMode
- IPConnQoSMaxAllowedPL
- IPConnQoSMaxAllowedDelay

7.8 Mapping PSTN Release Cause to SIP Response

The Mediant 1000 FXO module is used to interoperate between the SIP network and the PSTN/PBX. This interoperability includes the mapping of PSTN/PBX Call Progress Tones to SIP 4xx or 5xx responses for IP→Tel calls. The converse is also true: For Tel→IP calls, the SIP 4xx or 5xx responses are mapped to tones played to the PSTN/PBX.

When establishing an IP→Tel call, the following rules are applied:

- If the remote party (PSTN/PBX) is busy and the FXO gateway detects a Busy tone, it sends 486 Busy to IP. If it detects a Reorder tone, it sends 404 Not Found (no route to destination) to IP. In both cases the call is released. Note that if DisconnectOnBusyTone is set to 0, the FXO gateway ignores the detection of Busy/Reorder tones and doesn't release the call.
- For all other FXS/FXO release types (caused when there are no free channels in the specific trunk group, or when an appropriate rule for routing the call to a trunk group doesn't exist, or if the phone number isn't found), the gateway sends a SIP response (to IP) according to the parameter DefaultReleaseCause. This parameter defines Q.931 release causes. Its default value is '3', which is mapped to the SIP 404 response. By changing its value to '34', the SIP 503 response is sent. Other causes can be used as well.

7.9 Call Detail Record

The Call Detail Record (CDR) contains vital statistic information on calls made by the gateway. CDRs are generated at the end and (optionally) at the beginning of each call (determined by the parameter `CDRReportLevel`), and then sent to a Syslog server. The destination IP address for CDR logs is determined by the parameter `CDRSyslogServerIP`.

For CDR in RADIUS format, refer to 'Supported RADIUS Attributes' on page [402](#).

The following table lists the CDR fields that are supported.

Table 7-2: Supported CDR Fields

| Field Name | Description |
|-----------------|--|
| Cid | Port Number |
| CallId | SIP Call Identifier |
| Trunk | Physical Trunk Number (digital only) |
| BChan | Selected B-Channel (digital only) |
| ConId | SIP Conference ID |
| TG | Trunk Group Number |
| EPTyp | Endpoint Type |
| Orig | Call Originator (IP, Tel) |
| Sourcelp | Source IP Address |
| DestIp | Destination IP Address |
| TON | Source Phone Number Type |
| NPI | Source Phone Number Plan |
| SrcPhoneNum | Source Phone Number |
| SrcNumBeforeMap | Source Number Before Manipulation |
| TON | Destination Phone Number Type |
| NPI | Destination Phone Number Plan |
| DstPhoneNum | Destination Phone Number |
| DstNumBeforeMap | Destination Number Before Manipulation |
| Durat | Call Duration |
| Coder | Selected Coder |
| Intrv | Packet Interval |
| Rtplp | RTP IP Address |
| Port | Remote RTP Port |
| TrmSd | Initiator of Call Release (IP, Tel, Unknown) |
| TrmReason | Termination Reason |
| Fax | Fax Transaction during the Call |
| InPackets | Number of Incoming Packets |

Table 7-2: Supported CDR Fields

| Field Name | Description |
|-----------------|-------------------------------|
| OutPackets | Number of Outgoing Packets |
| PackLoss | Local Packet Loss |
| RemotePackLoss | Remote Packet Loss |
| Uniqueld | unique RTP ID |
| SetupTime | Call Setup Time |
| ConnectTime | Call Connect Time |
| ReleaseTime | Call Release Time |
| RTPdelay | RTP Delay |
| RTPjitter | RTP Jitter |
| RTPssrc | Local RTP SSRC |
| RemoteRTPssrc | Remote RTP SSRC |
| RedirectReason | Redirect Reason |
| TON | Redirection Phone Number Type |
| NPI | Redirection Phone Number Plan |
| RedirectPhonNum | Redirection Phone Number |

7.10 Supported RADIUS Attributes

Use the following table for explanations on the RADIUS attributes contained in the communication packets transmitted between the gateway and a RADIUS Server.

Table 7-3: Supported RADIUS Attributes

| Attribute Number | Attribute Name | VSA No. | Purpose | Value Format | Example | AAA ¹ |
|---------------------------|-----------------------|---------|---|-----------------------------|-----------------------|-----------------------|
| Request Attributes | | | | | | |
| 1 | User-Name | | Account number or calling party number or blank | String up to 15 digits long | 5421385747 | Start Acc Stop Acc |
| 4 | NAS-IP-Address | | IP address of the requesting gateway | Numeric | 192.168.14.43 | Start Acc Stop Acc |
| 6 | Service-Type | | Type of service requested | Numeric | 1: login | Start Acc Stop Acc |
| 26 | h323-incoming-conf-id | 1 | SIP call identifier | Up to 32 octets | | Start Acc Stop Acc |
| 26 | h323-remote-address | 23 | IP address of the remote gateway | Numeric | | Stop Acc |
| 26 | h323-conf-id | 24 | H.323/SIP call identifier | Up to 32 octets | | Start Acc Stop Acc |
| 26 | h323-setup-time | 25 | Setup time in NTP format 1 | String | | Start Acc Stop Acc |
| 26 | h323-call-origin | 26 | The call's originator: Answering (IP) or Originator (PSTN) | String | Answer, Originate etc | Start Acc Stop Acc |
| 26 | h323-call-type | 27 | Protocol type or family used on this leg of the call | String | VoIP | Start Acc Stop Acc |
| 26 | h323-connect-time | 28 | Connect time in NTP format | String | | Stop Acc |
| 26 | h323-disconnect-time | 29 | Disconnect time in NTP format | String | | Stop Acc |
| 26 | h323-disconnect-cause | 30 | Q.931 disconnect cause code | Numeric | | Stop Acc |
| 26 | h323-gw-id | 33 | Name of the gateway | String | SIPIDString | Start Acc Stop Acc |
| 26 | SIP-Call-ID | 34 | SIP Call ID | String | abcde@ac.com | Start Acc Stop Acc |
| 26 | Call-Terminator | 35 | The call's terminator: PSTN-terminated call (Yes); IP-terminated call (No). | String | Yes, No | Stop Acc |

Table 7-3: Supported RADIUS Attributes

| Attribute Number | Attribute Name | VSA No. | Purpose | Value Format | Example | AAA ¹ |
|----------------------------|---------------------|---------|---|--------------|--------------------|-----------------------|
| 30 | Called-Station-Id | | | String | 8004567145 | Start Acc |
| | | | Destination phone number | String | 2427456425 | Stop Acc |
| 31 | Calling-Station-Id | | Calling Party Number (ANI) | String | 5135672127 | Start Acc Stop Acc |
| 40 | Acct-Status-Type | | Account Request Type (start or stop) Note: 'start' isn't supported on the Calling Card application. | Numeric | 1: start, 2: stop | Start Acc Stop Acc |
| 41 | Acct-Delay-Time | | No. of seconds tried in sending a particular record | Numeric | 5 | Start Acc Stop Acc |
| 42 | Acct-Input-Octets | | Number of octets received for that call duration | Numeric | | Stop Acc |
| 43 | Acct-Output-Octets | | Number of octets sent for that call duration | Numeric | | Stop Acc |
| 44 | Acct-Session-Id | | A unique accounting identifier - match start & stop | String | 34832 | Start Acc Stop Acc |
| 46 | Acct-Session-Time | | For how many seconds the user received the service | Numeric | | Stop Acc |
| 47 | Acct-Input-Packets | | Number of packets received during the call | Numeric | | Stop Acc |
| 48 | Acct-Output-Packets | | Number of packets sent during the call | Numeric | | Stop Acc |
| 61 | NAS-Port-Type | | gateway physical port type on which the call is active | String | 0: Asynchronous | Start Acc Stop Acc |
| Response Attributes | | | | | | |
| 26 | h323-return-code | 103 | The reason for failing authentication (0 = ok, other number failed) | Numeric | 0 Request accepted | Stop Acc |
| 44 | Acct-Session-Id | | A unique accounting identifier – match start & stop | String | | Stop Acc |

7.10.1 RADIUS Server Messages

Below is an example of RADIUS Accounting, where the non-standard parameters are preceded with brackets.

```
Accounting-Request (361)
user-name = 111
acct-session-id = 1
nas-ip-address = 212.179.22.213
nas-port-type = 0
acct-status-type = 2
acct-input-octets = 4841
acct-output-octets = 8800
acct-session-time = 1
acct-input-packets = 122
acct-output-packets = 220
called-station-id = 201
calling-station-id = 202
// Accounting non-standard parameters:
(4923 33) h323-gw-id =
(4923 23) h323-remote-address = 212.179.22.214
(4923 1) h323-ivr-out = h323-incoming-conf-id:02102944 600a1899
3fd61009 0e2f3cc5
(4923 30) h323-disconnect-cause = 22 (0x16)
(4923 27) h323-call-type = VOIP
(4923 26) h323-call-origin = Originate
(4923 24) h323-conf-id = 02102944 600a1899 3fd61009 0e2f3cc5
```

7.11 Trunk-to-Trunk Routing Example

This example describes two gateways, each interfacing with the PSTN through four E1 spans. The gateway 'A' is configured to route all incoming Tel→IP calls to gateway 'B'. The gateway 'B' generates calls to PSTN on the same E1 trunk as the call was originally received (in gateway 'A').

- gateway 'A' IP address: 192.168.3.50
- gateway 'B' IP address: 192.168.3.51

The ini file parameters configuration for gateways 'A' and 'B' include the following:

1. Define, for both gateways, four trunk groups, each with 30 B-channels:
 - TrunkGroup_1 = 0/1-31,1000
 - TrunkGroup_2 = 1/1-31,2000
 - TrunkGroup_3 = 2/1-31,3000
 - TrunkGroup_4 = 3/1-31,4000
2. In gateway 'A', add the originating Trunk Group ID as a prefix to the destination number for Tel→IP calls:
AddTrunkGroupAsPrefix = 1
3. In gateway 'A', route all incoming PSTN calls, starting with the prefixes 1, 2, 3, and 4, to gateway's 'B' IP address:
 - Prefix = 1, 192.168.3.51
 - Prefix = 2, 192.168.3.51

- Prefix = 3, 192.168.3.51
- Prefix = 4, 192.168.3.51

Note: It is also possible to define Prefix = *,192.168.3.51 instead of the four lines above.

4. In gateway 'B', route IP→PSTN calls to Trunk Group ID according to the first digit of the called number:
 - PSTNPrefix = 1,1
 - PSTNPrefix = 2,2
 - PSTNPrefix = 3,4
 - PSTNPrefix = 4,4
5. In gateway 'B', remove the first digit from each IP→PSTN number before it is used in an outgoing call:
 NumberMapIP2Tel = *,1

7.12 Proxy or Registrar Registration Example

Below is an example of Proxy and Registrar Registration:

```
REGISTER sip:servername SIP/2.0
VIA: SIP/2.0/UDP 212.179.22.229;branch=z9hG4bRaC7AU234
From: <sip:GWRegistrationName@sipgatewayname>;tag=1c29347
To: <sip:GWRegistrationName@sipgatewayname>
Call-ID: 10453@212.179.22.229
Seq: 1 REGISTER
Expires: 3600
Contact: sip:GWRegistrationName@212.179.22.229
Content-Length: 0
```

The 'servername' string is defined according to the following rules:

- The "servername" is equal to "RegistrarName" if configured. The "RegistrarName" can be any string.
- Otherwise, the "servername" is equal to "RegistrarIP" (either FQDN or numerical IP address), if configured.
- Otherwise, the "servername" is equal to "ProxyName" if configured. The "ProxyName" can be any string.
- Otherwise, the "servername" is equal to "ProxyIP" (either FQDN or numerical IP address).

The parameter GWRegistrationName can be any string. This parameter is used only if registration is Per Gateway. If the parameter is not defined, the parameter UserName is used instead. If the registration is per endpoint, the endpoint phone number is used.

The 'sipgatewayname' parameter (defined in the *ini* file or Embedded Web Server), can be any string. Some Proxy servers require that the 'sipgatewayname' (in REGISTER messages) is set equal to the Registrar / Proxy IP address or to the Registrar / Proxy domain name. The 'sipgatewayname' parameter can be overwritten by the TrunkGroupSettings_GatewayName value if the TrunkGroupSettings_RegistrationMode is set to "Per Endpoint".

REGISTER messages are sent to the Registrar's IP address (if configured) or to the Proxy's IP address. A single message is sent once per gateway, or messages are sent per B-channel according to the parameter AuthenticationMode. There is also an option to configure registration mode per Trunk Group using the TrunkGroupSettings table. The registration request is resent according to the parameter RegistrationTimeDivider. For example, if RegistrationTimeDivider = 70 (%) and Registration Expires time = 3600, the gateway resends its registration request after $3600 \times 70\% = 2520$ sec. The default value of RegistrationTimeDivider is 50%.

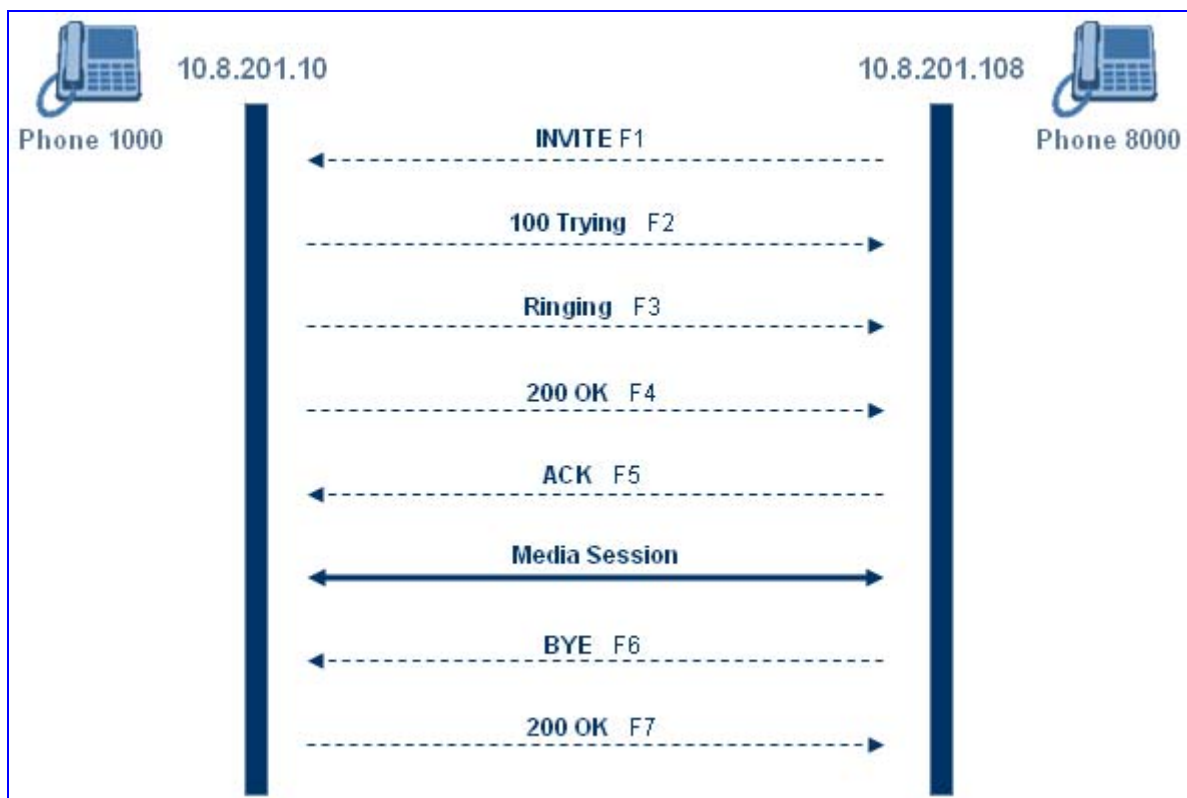
If registration per B-channel is selected, on gateway startup the gateway sends REGISTER requests according to the maximum number of allowed SIP dialogs (configured by the parameter NumberOfActiveDialogs). After each received response, the subsequent REGISTER request is sent.

7.13 Configuration Examples

7.13.1 SIP Call Flow

The SIP call flow (shown in the following figure), describes SIP messages exchanged between two gateways during a simple call. In this call flow example, gateway (10.8.201.158) with phone number '6000' dials gateway (10.8.201.161) with phone number '2000'.

Figure 7-4: SIP Call Flow



■ F1 (10.8.201.108 >> 10.8.201.10 INVITE):

```
INVITE sip:1000@10.8.201.10;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
CSeq: 18153 INVITE
Contact: <sip:8000@10.8.201.108;user=phone>
User-Agent: Audiocodes-Sip-Gateway/MP-108 FXS/v.4.20.299.410
Supported: 100rel,em
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,
NOTIFY,PRACK,REFER,INFO
Content-Type: application/sdp
Content-Length: 208

v=0
o=AudiocodesGW 18132 74003 IN IP4 10.8.201.108
s=Phone-Call
c=IN IP4 10.8.201.108
t=0 0
m=audio 4000 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

■ F2 (10.8.201.10 >> 10.8.201.108 TRYING):

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
Server: Audiocodes-Sip-Gateway/TrunkPack 1610/v.4.20.299.412
CSeq: 18153 INVITE
Content-Length: 0
```

■ F3 (10.8.201.10 >> 10.8.201.108 180 RINGING):

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
Server: Audiocodes-Sip-Gateway/TrunkPack 1610/v.4.20.299.412
CSeq: 18153 INVITE
Supported: 100rel,em
Content-Length: 0
```



Note: Phone '1000' answers the call and then sends a 200 OK message to gateway 10.8.201.108.

■ **F4 (10.8.201.10 >> 10.8.201.108 200 OK):**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
CSeq: 18153 INVITE
Contact: <sip:1000@10.8.201.10;user=phone>
Server: Audiocodes-Sip-Gateway/TrunkPack 1610/v.4.20.299.412
Supported: 100rel,em
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,
NOTIFY,PRACK,REFER,INFO
Content-Type: application/sdp
Content-Length: 206

v=0
o=AudiocodesGW 30221 87035 IN IP4 10.8.201.10
s=Phone-Call
c=IN IP4 10.8.201.10
t=0 0
m=audio 7210 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=ptime:20
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
```

■ **F5 (10.8.201.108 >> 10.8.201.10 ACK):**

```
ACK sip:1000@10.8.201.10;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacZYpJWxZ
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
User-Agent: Audiocodes-Sip-Gateway/MP-108 FXS/v.4.20.299.410
CSeq: 18153 ACK
Supported: 100rel,em
Content-Length: 0
```



Note: Phone '8000' goes on-hook and gateway 10.8.201.108 sends a BYE to gateway 10.8.201.10. Voice path is established.

■ **F6 (10.8.201.108 >> 10.8.201.10 BYE):**

```
BYE sip:1000@10.8.201.10;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacRKCVBud
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
User-Agent: Audiocodes-Sip-Gateway/MP-108 FXS/v.4.20.299.410
CSeq: 18154 BYE
Supported: 100rel,em
Content-Length: 0
```

■ **F7 (10.8.201.10 >> 10.8.201.108 200 OK):**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacRKCVBud
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
Server: Audiocodes-Sip-Gateway/TrunkPack 1610/v.4.20.299.412
CSeq: 18154 BYE
Supported: 100rel,em
Content-Length: 0
```

7.13.2 SIP Authentication Example

The gateway supports basic and digest (MD5) authentication types, according to SIP RFC 3261 standard. A proxy server might require authentication before forwarding an INVITE message. A Registrar/Proxy server may also require authentication for client registration. A proxy replies to an unauthenticated INVITE with a 407 Proxy Authorization Required response, containing a Proxy-Authenticate header with the form of the challenge. After sending an ACK for the 407, the user agent can then resend the INVITE with a Proxy-Authorization header containing the credentials.

User agent, redirect or registrar servers typically use 401 Unauthorized response to challenge authentication containing a WWW-Authenticate header, and expect the re-INVITE to contain an Authorization header.

The following example describes the Digest Authentication procedure including computation of user agent credentials.

1. The REGISTER request is sent to Registrar/Proxy server for registration, as follows:

```
REGISTER sip:10.2.2.222 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.200
From: <sip:122@10.1.1.200>;tag=1c17940
To: <sip:122@10.1.1.200>
Call-ID: 634293194@10.1.1.200
User-Agent: Audiocodes-Sip-Gateway/gateway/v.4.20.299.410
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
```

2. Upon receipt of this request, the Registrar/Proxy returns 401 Unauthorized response.

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 10.2.1.200
From: <sip:122@10.2.2.222 >;tag=1c17940
To: <sip:122@10.2.2.222 >
Call-ID: 634293194@10.1.1.200
Cseq: 1 REGISTER
Date: Mon, 30 Jul 2001 15:33:54 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0

WWW-Authenticate: Digest realm="audiocodes.com",
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
stale=FALSE,
algorithm=MD5
```

3. According to the sub-header present in the WWW-Authenticate header the correct REGISTER request is formed.
 4. Since the algorithm used is MD5, then:
 - The username is equal to the endpoint phone number: 122
 - The realm return by the proxy: audiocodes.com
 - The password from the *ini* file: AudioCodes.
 - The equation to be evaluated: (according to RFC this part is called A1): **'122:audiocodes.com:AudioCodes'**.
 - The MD5 algorithm is run on this equation and stored for future usage.
 - The result is: 'a8f17d4b41ab8dab6c95d3c14e34a9e1'
 5. Next, the par called A2 needs to be evaluated:
 - The method type is 'REGISTER'.
 - Using SIP protocol 'sip'.
 - Proxy IP from *ini* file is '10.2.2.222'.
 - The equation to be evaluated: **'REGISTER:sip:10.2.2.222'**.
 - The MD5 algorithm is run on this equation and stored for future usage.
 - The result is: 'a9a031cfddcb10d91c8e7b4926086f7e'
 6. The final stage:
 - The A1 result: The nonce from the proxy response is '11432d6bce58ddf02e3b5e1c77c010d2'.
 - The A2 result: The equation to be evaluated is **'A1:11432d6bce58ddf02e3b5e1c77c010d2:A2'**.
 - The MD5 algorithm is run on this equation. The outcome of the calculation is the response needed by the gateway to register with the Proxy.
 - The response is: 'b9c45d0234a5abf5ddf5c704029b38cf'
- At this time a new REGISTER request is issued with the response:

```
REGISTER sip:10.2.2.222 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c23940
To: <sip: 122@10.1.1.200>
Call-ID: 654982194@10.1.1.200
Server: Audiocodes-Sip-Gateway/Mediant 1000/v.4.20.299.410
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
Authorization: Digest, username: 122,
realm="audiocodes.com",
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
uri="10.2.2.222",
response="b9c45d0234a5abf5ddf5c704029b38cf"
```

7. Upon receiving this request and if accepted by the Proxy, the proxy returns a 200 OK response closing the REGISTER transaction.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c23940
To: <sip: 122@10.1.1.200>
Call-ID: 654982194@10.1.1.200
Cseq: 1 REGISTER
Date: Thu, 26 Jul 2001 09:34:42 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0
Contact: <sip:122@10.1.1.200>; expires="Thu, 26 Jul 2001 10:34:42 GMT"; action=proxy; q=1.00
Contact: <122@10.1.1.200>; expires="Tue, 19 Jan 2038 03:14:07 GMT"; action=proxy; q=0.00
Expires: Thu, 26 Jul 2001 10:34:42 GMT
```

7.13.3 Establishing a Call between Two gateways

After you've installed and set up the gateway, you can ensure that it functions as expected by establishing a call between it and another gateway. This section describes how to configure two 4-port Mediant 1000 FXS SIP gateway to establish a call. After configuration, you can make calls between telephones connected to a single Mediant 1000 gateway or between the two Mediant 1000 gateways.

In the following example, the IP address of the first gateway is 10.2.37.10 and its endpoint numbers are 101 to 104. The IP address of the second gateway is 10.2.37.20 and its endpoint numbers are 201 to 204.

In this example, a SIP Proxy is not used. Internal call routing is performed using the internal 'Tel to IP Routing' table.

➤ **To configure the two gateways, take these 4 steps:**

1. For the *first* gateway (10.2.37.10), in the 'Trunk Group Table' screen (**Protocol Management** menu > Trunk Group), assign the phone numbers 101 to 104 for the gateway's endpoints.

| Group Index | Module | From Trunk | To Trunk | Channels | Phone Number | Trunk Group ID | Profile ID |
|-------------|--------------|------------|----------|----------|--------------|----------------|------------|
| 1 | Module 3 FXS | 1 | 1 | 1-4 | 101 | 0 | 0 |

2. For the *second* gateway (10.2.37.20), in the 'Trunk Group Table' screen, assign the phone numbers 201 to 204 for the gateway's endpoints.

Figure 7-5: Assigning Phone Numbers

| Group Index | Module | From Trunk | To Trunk | Channels | Phone Number | Trunk Group ID | Profile ID |
|-------------|--------------|------------|----------|----------|--------------|----------------|------------|
| 1 | Module 3 FXS | 1 | 1 | 1-4 | 201 | 0 | 0 |

3. Configure the following settings for *both* gateways:

In the 'Tel to IP Routing' screen (**Protocol Management** menu > **Routing Tables** submenu > **Tel to IP Routing**), in the first row, enter 10 in the 'Destination Phone Prefix' field and enter the IP address of the first gateway (10.2.37.10) in the field 'IP Address'. In the second row, enter 20 and the IP address of the second gateway (10.2.37.20) respectively.

These settings enable the routing (from both gateways) of outgoing Tel→IP calls that start with 10 to the first gateway and calls that start with 20 to the second gateway.

Figure 7-6: Tel to IP Routing Screen

| | Dest. Phone Prefix | Source Phone Prefix | Dest. IP Address | Profile ID | Status |
|---|--------------------|---------------------|------------------|------------|--------|
| 1 | 10 | * | 10.2.37.10 | 0 | n/a |
| 2 | 20 | * | 10.2.37.20 | 0 | n/a |

4. Make a call. Pick up the phone connected to port #1 of the first gateway and dial 102 (to the phone connected to port #2 of the same gateway). Listen for progress tones at the calling endpoint and for ringing tone at the called endpoint. Answer the called endpoint, speak into the calling endpoint, and check the voice quality. Dial 201 from the phone connected to port #1 of the first gateway; the phone connected to port #1 of the second gateway rings. Answer the call and check the voice quality.

7.13.4 Remote IP Extension between FXO and FXS

This application explains how to implement remote extension via IP, using -port FXO and-port FXS Mediant 1000 gateways. In this configuration, PBX incoming calls are routed to the 'Remote Extension' via the FXO and FXS modules.

Requirements:

- One FXO Mediant 1000 gateway
- One FXS Mediant 1000 gateway
- Analog phones (POTS)
- PBX – one or more PBX loop start lines
- LAN

Connect the FXO Mediant 1000 ports directly to the PBX lines, as shown in the diagram, below:

7.13.4.1 Dialing from Remote Extension (Phone Connected to FXS)

➤ **To configure the call, take these 3 steps:**

1. Lift the handset to listen to the dial tone from the PBX, as if the phone was connected directly to the PBX. The FXS and FXO Mediant 1000 gateways establish a voice path connection from the phone to the PBX immediately after the phone handset is raised.
2. Dial the destination number (the DTMF digits are sent, over IP, directly to the PBX). All tones heard are generated from the PBX (such as Ringback, busy or fast busy tones). There is one-to-one mapping between FXS ports and PBX lines.
3. The call is disconnected when the phone connected to the FXS goes onhook.

7.13.4.2 Dialing from other PBX line, or from PSTN

➤ **To configure the call, take these 5 steps:**

1. Dial the PBX subscriber number in the same way as if the user's phone was connected directly to the PBX.
2. As soon as the PBX rings the FXO gateway, the ring signal is 'sent' to the phone connected to the FXS gateway.
3. Once the phone's handset, connected to the Mediant 1000 FXS is raised, the Mediant 1000 FXO seizes the PBX line and the voice path is established between the phone and the PBX line.
4. There is a one-to-one mapping between PBX lines and FXS Mediant 1000 ports. Each PBX line is routed to the same phone (connected to FXS Mediant 1000).
5. The call is disconnected when the phone that is connected to FXS Mediant 1000 goes onhook.

7.13.4.3 FXS Gateway Configuration (using the Embedded Web Server)

➤ **To configure the FXS gateway, take these 3 steps:**

1. In the 'Endpoint Phone Numbers' screen, assign the phone numbers 100 to 107 for the gateway's endpoints.

Figure 7-7: Endpoint Phone Number Screen

| Group Index | Module | From Trunk | To Trunk | Channels | Phone Number | Trunk Group ID | Profile ID |
|-------------|--------------|------------|----------|----------|--------------|----------------|------------|
| 1 | Module 3 FXS | 1 | 1 | 1-4 | 100 | 0 | 0 |

2. In the 'Automatic Dialing' screen, enter the phone numbers of the FXO gateway in the 'Destination Phone Number' fields. When a phone connected to port #1 goes offhook, the FXS gateway automatically dials the number '200'.

Figure 7-8: Automatic Dialing Screen

| Automatic Dialing | | | |
|---------------------|--------------------------|------------------|---|
| Gateway Port | Destination Phone Number | Auto Dial Status | |
| Module 3 Port 1 FXS | 200 | Enable | ▼ |
| Module 3 Port 2 FXS | 201 | Enable | ▼ |
| Module 3 Port 3 FXS | 202 | Enable | ▼ |
| Module 3 Port 4 FXS | 203 | Enable | ▼ |

3. In the 'Tel to IP Routing' screen, enter 20 in the 'Destination Phone Prefix' field, and the IP address of the FXO gateway (10.1.10.2) in the field 'IP Address'.

Figure 7-9: Tel to IP Routing Screen

| | Dest. Phone Prefix | Source Phone Prefix | Dest. IP Address | Profile ID | Status |
|---|--------------------|---------------------|------------------|------------|--------|
| 1 | 20 | * | 10.1.10.2 | 0 | n/a |



Note: In remote extensions, for the transfer to function, Hold must be disabled on the FXS gateway (i.e., Enable Hold = 0) and hook-flash must be transferred from the FXS to the FXO (HookFlashOption = 4).

7.13.4.4 FXO Gateway Configuration (using the Embedded Web Server)

➤ **To configure the FXO Mediant 1000, take these 4 steps:**

1. In the 'Endpoint Phone Numbers' screen, assign the phone numbers 200 to 207 for the gateway's endpoints.

Figure 7-10: Endpoint Phone Number Screen

| Group Index | Module | From Trunk | To Trunk | Channels | Phone Number | Trunk Group ID | Profile ID |
|-------------|--------------|------------|----------|----------|--------------|----------------|------------|
| 1 | Module 2 FXO | 1 | 1 | 1-4 | 200 | | 0 |

2. In the 'Automatic Dialing' screen, enter the phone numbers of the FXS gateway in the 'Destination Phone Number' fields. When a ringing signal is detected at port #1, the FXO gateway automatically dials the number '100'.

Figure 7-11: Automatic Dialing Screen

| Automatic Dialing | | | |
|---------------------|--------------------------|------------------|---|
| Gateway Port | Destination Phone Number | Auto Dial Status | |
| Module 2 Port 1 FXO | 100 | Enable | ▼ |
| Module 2 Port 2 FXO | 101 | Enable | ▼ |
| Module 2 Port 3 FXO | 102 | Enable | ▼ |
| Module 2 Port 4 FXO | 103 | Enable | ▼ |

3. In the 'Tel to IP Routing' screen, enter 10 in the 'Destination Phone Prefix' field, and the IP address of the FXS gateway (10.1.10.3) in the field 'IP Address'.

Figure 7-12: Tel to IP Routing Screen

| | Dest. Phone Prefix | Source Phone Prefix | Dest. IP Address | Profile ID | Status |
|---|--------------------|---------------------|------------------|------------|--------|
| 1 | 10 | * | 10.1.10.3 | 0 | n/a |

4. In the 'Protocol Management' screen, set the parameter 'Dialing Mode' to 'Two Stage' (IsTwoStageDial = 1).

7.14 Working with Supplementary Services

The gateway supports the following supplementary services:

- Call Hold and Retrieve; refer to 'Call Hold and Retrieve' on page 415
- Consultation / Alternate; refer to 'Consultation / Alternate' on page 416
- Call Transfer; refer to 'Call Transfer' on page 416
- Call Forward (3xx Redirect Responses); refer to 'Call Forward' on page 417
- Call Waiting (182 Queued Response); refer to 'Call Waiting' on page 418
- Message Waiting Indication (MWI); refer to 'Message Waiting Indication' on page 418
- Caller ID (refer to 'Caller ID' on page 419)

To activate these supplementary services (Hold, Transfer, Forward, Waiting and MWI) on the gateway, enable each service's corresponding parameter either from the Embedded Web Server or via the ini file.



Notes:

- All call participants must support the specific supplementary service that is used.
- When working with certain application servers (such as BroadSoft's BroadWorks) in client server mode (the application server controls all supplementary services and keypad features by itself), the gateway's supplementary services must be disabled.

7.14.1 Call Hold and Retrieve

Initiating Hold / Retrieve:

- Active calls can be put on-hold by pressing the phone's hook-flash button.
- The party that initiates the hold is called the *holding* party; the other party is called the *held* party.
- After a successful Hold, the holding party hears a Dial Tone (HELD_TONE, defined in the gateway's Call Progress Tones file).
- Call retrieve can be performed only by the holding party while the call is held and active.
- The holding party performs the retrieve by pressing the hook-flash.
- After a successful retrieve, the voice is connected again.
- Hold is performed by sending REINVITE message with IP address 0.0.0.0 or a=sendonly in the SDP according to the parameter HoldFormat.

- The hold and retrieve functionalities are implemented by REINVITE messages. The IP address 0.0.0.0 as the connection IP address or the string 'a=inactive' in the received Re-INVITE SDP cause the gateway to enter Hold state and to play held tone (configured in the gateway) to the PBX/PSTN. If the string 'a=sendonly' is received in the SDP message, the gateway stops sending RTP packets, but continues to listen to the incoming RTP packets. Usually, the remote party plays, in this scenario, Music on Hold (MOH) and the gateway forwards the MOH to the held party.

Receiving Hold / Retrieve

- When an active call receives Re-INVITE message with either the IP address 0.0.0.0 or the 'inactive' string in SDP, the gateway stops sending RTP and plays a local Held Tone.
- When an active call receives Re-INVITE message with 'sendonly' string in SDP, the gateway stops sending RTP and listens to the remote party. In this mode, it is expected that on-hold music (or any other hold tone) is to be played (over IP) by the remote party.

7.14.2 Consultation / Alternate

- The consultation feature is relevant only for the holding party (applicable only to the FXS module).
- After holding a call (by pressing hook-flash), the holding party hears a dial tone and can now initiate a new call, which is called a consultation call.
- While hearing a dial tone, or when dialing to the new destination (before dialing is complete), the user can retrieve the held call by pressing hook-flash.
- The held call can't be retrieved while Ringback tone is heard.
- After the consultation call is connected, the user can switch between the held and active call by pressing hook-flash.

7.14.3 Call Transfer

There are two types of call transfers:

- **Consultation Transfer** (REFER and REPLACES):

The common way to perform a consultation transfer is as follows:

In the transfer scenario there are three parties: Party A = transferring, Party B = transferred, Party C = transferred to.

- A Calls B.
- B answers.
- A presses the hook-flash and puts B on-hold (party B hears a hold tone).
- A dials C.
- After A completes dialing C, A can perform the transfer by on-hooking the A phone.
- After the transfer is complete, B and C parties are engaged in a call.

The transfer can be initiated at any of the following stages of the call between A and C:

- Just after completing dialing C phone number - transfer from setup.
- While hearing Ringback – transfer from alert.
- While speaking to C - transfer from active.

■ **Blind Transfer (REFER):**

Blind transfer is performed after we have a call between A and B, and party A decides to immediately transfer the call to C without speaking with C. The result of the transfer is a call between B and C (just like consultation transfer only skipping the consultation stage).

Note the following SIP issues:

- Transfer is initiated by sending REFER with REPLACES.
- The gateway can receive and act upon receiving REFER with or without REPLACES.
- The gateway can receive and act upon receiving INVITE with REPLACES, in which case the old call is replaced by the new one.
- The INVITE with REPLACES can be used to implement Directed Call Pickup.

7.14.4 Call Forward

Five forms of call forward are supported:

- **Immediate:** incoming call is forwarded immediately and unconditionally.
- **Busy:** incoming call is forwarded if the endpoint is busy.
- **No Reply:** incoming call is forwarded if it isn't answered for a specified time.
- **On Busy or No Reply:** incoming call is forwarded if the port is busy or when calls are not answered after a specified time.
- **Do Not Disturb:** immediately reject incoming calls. Upon receiving a call to Do Not Disturb call, the 603 Decline SIP response code is sent.

Three forms of forwarding parties are available:

- **Served party:** the party that is configured to forward the call (FXS gateway)
- **Originating party:** the party that initiated the first call (FXS or FXO gateway)
- **Diverted party:** the new destination of the forwarded call (FXS or FXO gateway)

The served party (FXS gateway) can be configured through the Embedded Web Server (refer to 'Call Forward' on page 157) or via *ini* file to activate one of the call forward modes. These modes are configurable per gateway endpoints.

Note the following SIP issues:

- **Initiating forward:** When forward is initiated, the gateway sends a 302 response with a contact that contains the phone number from the forward table and its corresponding IP address from the routing table (or, when Proxy is used, the proxy's IP address).
- **Receiving forward:** The gateway handles 3xx responses for redirecting calls with a new contact.

7.14.5 Call Waiting

The Call Waiting feature enables FXS gateway to accept an additional (second) call on busy endpoints. If an incoming IP call is designated to a busy port, the called party hears call waiting tone (several configurable short beeps) and (for Bellcore and ETSI Caller IDs) can view the Caller ID string of the incoming call. The calling party hears a Call Waiting Ringback Tone. The called party can accept the new call using hook-flash, and can toggle between the two calls.

To enable Call Waiting:

- Set EnableCallWaiting = 1 (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)
- Set EnableHold = 1.
- Define the Call Waiting indication and Call Waiting Ringback tones in the Call Progress Tones file. You can define up to four Call Waiting indication tones (refer to the parameter FirstCallWaitingToneID in 'SIP Configuration Parameters' on page 323).
- To configure the Call Waiting indication tone cadence, modify the following parameters: NumberOfWaitingIndications, WaitingBeepDuration and TimeBetweenWaitingIndications (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113).
- To configure a delay interval before a Call Waiting Indication is played to the currently busy port use the parameter TimeBeforeWaitingIndication (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113). This enables the caller to hang up before disturbing the called party with Call Waiting Indications. Applicable only to FXS modules.

Both the calling and called sides are supported by FXS modules; the FXO modules support only the calling side.

To indicate Call Waiting, the gateway sends a 182 Call Queued response. The gateway identifies a Waiting Call when a 182 Call Queued response is received.

7.14.6 Message Waiting Indication

Support for Message Waiting Indication (MWI) according to IETF <draft-ietf-sipping-mwi-04.txt>, including SUBSCRIBE (to MWI server). The FXS gateway can accept an MWI NOTIFY message that indicates waiting messages or that the MWI is cleared. Users are informed of these messages by a stutter dial tone. The stutter and confirmation tones are defined in the CPT file (refer to Configuring the Call Progress Tones File in the *Reference Manual*). If the MWI display is configured, the number of waiting messages is also displayed. If the MWI lamp is configured, the phone's lamp (on a phone that is equipped with an MWI lamp) is lit. The gateway can subscribe to the MWI server per port (usually used on FXS) or per gateway (used on FXO).

To configure MWI, set the following parameters:

- EnableMWI (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)
- MWIServerIP (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)
- MWIAnalogLamp (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)
- MWIDisplay (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)

- StutterToneDuration (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)
- EnableMWISubscription (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)
- MWIExpirationTime (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)
- SubscribeRetryTime (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)
- SubscriptionMode (or using the Embedded Web Server, refer to 'Proxy & Registration Parameters' on page 84)
- CallerIDType -- determines the standard for detection of MWI signals (or using the Embedded Web Server, refer to 'Supplementary Services' on page 113)
- ETSIVMWITypeOneStandard (for a description, refer to 'Analog Telephony Parameters' on page 350)
- BellcoreVMWITypeOneStandard (for a description, refer to 'Analog Telephony Parameters' on page 350)

7.14.7 Caller ID

This section discusses the gateway's Caller ID support for analog modules.

7.14.7.1 Caller ID Detection / Generation on the Tel Side

By default, generation and detection of Caller ID to the Tel side is disabled. To enable Caller ID, set the parameter EnableCallerID to 1. When the Caller ID service is enabled:

- For FXS: the Caller ID signal is sent to the gateway's port
- For FXO: the Caller ID signal is detected

The configuration for Caller ID is described below:

- Use the parameter CallerIDType to define the Caller ID standard. Note that the Caller ID standard that is used on the PBX or phone must match the standard defined in the gateway.
- Select the Bellcore caller ID sub standard using the parameter BellcoreCallerIDTypeOneSubStandard
- Select the ETSI FSK caller ID sub standard using the parameter ETSICallerIDTypeOneSubStandard
- Enable or disable (per port) the caller ID generation (for FXS gateways) and detection (for FXO gateways) using the 'Generate / Detect Caller ID to Tel' table (EnableCallerID). If a port isn't configured, its caller ID generation / detection are determined according to the global parameter EnableCallerID.
- EnableCallerIDTypeTwo: disables / enables the generation of Caller ID type 2 when the phone is off-hooked (used for call waiting).
- RingsBeforeCallerID: sets the number of rings before the gateway starts detection of caller ID (FXO only). By default, the gateway detects the caller ID signal between the first and second rings.

- **AnalogCallerIDTimingMode:** determines the time period when a caller ID signal is generated (FXS only). By default, the caller ID is generated between the first two rings.
- **PolarityReversalType:** some Caller ID signals use reversal polarity and/or wink signals. In these scenarios, it is recommended to set **PolarityReversalType** to 1 (Hard) (FXS only).
- The Caller ID interworking can be changed using the parameters **UseSourceNumberAsDisplayName** and **UseDisplayNameAsSourceNumber**.

7.14.7.2 Debugging a Caller ID Detection on FXO

➤ **To debug a Caller ID detection on an FXO gateway, take these 6 steps:**

1. Verify that the parameter **EnableCallerID** is set to 1.
2. Verify that the caller ID standard (and substandard) of the gateway match the standard of the PBX (**CallerIDType**, **BellcoreCallerIDTypeOneSubStandard**, and **ETSICallerIDTypeOneSubStandard**).
3. Define the number of rings before the gateway starts detection of caller ID (**RingsBeforeCallerID**).
4. Verify that the coefficient file that is loaded on the gateway is correct (if the caller ID signal is distorted, the gateway won't recognize it).
5. Connect a phone to the analog line of the PBX (instead of the FXO gateway) and verify that it displays the caller ID.
6. Record the caller ID signal and send it to R&D.

To record the signal:

- a. Change the software version of the gateway to an MGCP version.
- b. Configure the following parameters:
 - ◆ **MGCPDefaultCoder** = 'X-CCD'
 - ◆ **ActivateallChannelsOnBoardInit** = 1
 - ◆ **DTMFTransportType** = 2
 - ◆ **MFTransportType** = 2
 - ◆ **CallerIDTransportType** = 0
 - ◆ **FaxTransportMode** = 0
 - ◆ **V22ModemTransportType** = 0
 - ◆ **V23ModemTransportType** = 0
 - ◆ **V32ModemTransportType** = 0
 - ◆ **V34ModemTransportType** = 0
- c. Reset the gateway.
- d. Start the DSP recording.

7.14.7.3 Caller ID on the IP Side

7.14.7.3.1 Overview

Caller ID is provided by the From header containing the caller's name and "number", for example:

```
From: "David" <SIP:101@10.33.2.2>;tag=35dfsgasd45dg
```

If Caller ID is restricted (received from Tel or configured in the gateway), the From header is set to:

```
From: "anonymous" <anonymous@anonymous.invalid>; tag=35dfsgasd45dg
```

The P-asserted (or P-preferred) headers are used to present the originating party's caller ID even when the caller ID is restricted. These headers are used together with the Privacy header.

- If Caller ID is restricted:
 - The From header is set to "anonymous" <anonymous@anonymous.invalid>
 - The 'Privacy: id' header is included
 - The P-Asserted-Identity (or P-preferred-Identity) header shows the caller ID
- If Caller ID is allowed:
 - The From header shows the caller ID
 - The 'Privacy: none' header is included
 - The P-Asserted-Identity (or P-preferred-Identity) header shows the caller ID

In addition, the caller ID (and presentation) can be displayed in the Calling Remote-Party-ID header.

7.14.7.3.2 Configuration

The 'Caller Display Information' table (CallerDisplayInfo) is used:

- For FXS modules: to define the caller ID (per port) that is sent to IP.
- For FXO modules: to define the caller ID (per port) that is sent to IP if caller ID isn't detected on the Tel side, or when EnableCallerID = 0.
- For both FXS and FXO modules: to determine the presentation of the caller ID (allowed or restricted)
- To maintain backward compatibility: when the strings 'Private' or 'Anonymous' are set in the Caller ID/Name field, the caller ID is restricted and the value in the Presentation field is ignored.

The value of the 'Presentation' field that is defined in the 'Caller Display Information' table can be overridden by configuring the 'Presentation' parameter in the 'Tel to IP Source Number Manipulation' table. Therefore, this table can be used to set the presentation for specific calls according to Source / Destination prefixes.

The caller ID can be restricted / allowed (per port) using keypad features KeyCLIR and KeyCLIRDeact (FXS only).

AssertedIdMode defines the header that is used (in the generated INVITE request) to deliver the caller ID (P-Asserted-Identity or P-preferred-Identity). Use the parameter UseTelURIForAssertedID to determine the format of the URI in these headers (sip: or tel:).

EnableRPIheader enables Remote-Party-ID (RPI) headers for calling and called numbers for Tel-to-IP calls.

8 Networking Capabilities

8.1 Ethernet Interface Configuration

The Ethernet connection mode can be controlled by using the *ini* file parameter `EthernetPhyConfiguration` to configure one of the following modes:

- Manual modes (10 Base-T Half-Duplex, 10 Base-T Full-Duplex, 100 Base-TX Half-Duplex, 100 Base-TX Full-Duplex)
- Auto-Negotiate mode

Auto-Negotiation falls back to Half-Duplex mode when the opposite port is not Auto-Negotiate, but the speed (i.e., 10/100 Base-T) in this mode is always configured correctly. Note that configuring the gateway to Auto-Negotiate mode while the opposite port is set manually to Full-Duplex (either 10 Base-T or 100 Base-T) is invalid (as it causes the gateway to fall back to Half-Duplex mode while the opposite port is Full-Duplex). It's also invalid to set the gateway to one of the manual modes while the opposite port is either Auto-Negotiate or not exactly matching (both in speed and in duplex mode). It's recommended to always prefer Full-Duplex connections to Half-Duplex ones and 100 Base-TX to 10 Base-T (due to the larger bandwidth). It's also strongly recommended to use the same mode in both link partners. Any mismatch configuration can yield unexpected functioning of the Ethernet connection.

Note that when remote configuration is performed, the gateway should be in the correct Ethernet setting prior to the time this parameter takes effect. When, for example, the gateway is configured using BootP/TFTP, the gateway must perform many Ethernet-based transactions prior to reading the *ini* file containing this gateway configuration parameter.

To resolve this problem, the gateway always uses the last Ethernet setup mode configured. In this way, if you want to configure the gateway to operate in a new network environment in which the current Ethernet setting of the gateway is invalid, you should first modify this parameter in the current network so that the new setting holds next time the gateway is restarted. After reconfiguration has completed, connect the gateway to the new network and restart it. As a result, the remote configuration process that takes place in the new network uses a valid Ethernet configuration.

8.2 Ethernet Interface Redundancy

The Mediant 1000 supports Ethernet redundancy by providing two Ethernet ports, located on the CPU module. The Ethernet port redundancy feature is enabled using the *ini* file parameter `MIIRedundancyEnable`. By default, this feature is disabled.

When Ethernet redundancy is implemented, the two Ethernet ports can be connected to the same switch (segment / hub). In this setup, one Ethernet port is active and the other is redundant. If an Ethernet connection failure is detected, the CPU module switches over to the redundant Ethernet port. The CPU issues a Major alarm that displays 'Redundant Link (Physical port #1) is down', indicating the failed physical port.

If the first Ethernet port connection is restored, the Major alarm is cleared, displaying 'Alarm cleared: Redundant Link (Physical port #1) is up'. The first physical port now becomes the redundant port in case of failure with the active physical port (which is currently the second physical port).

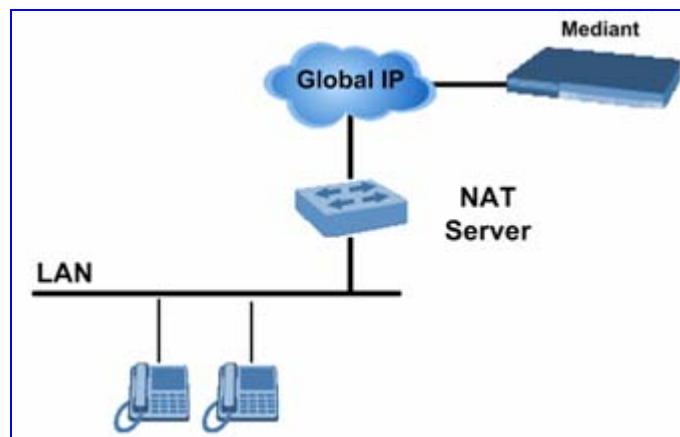
When the CPU module loses all Ethernet connectivity, a Critical alarm is generated (displaying 'No Ethernet Link'):

- When MIIRedundancyEnable is disabled: the alarm is generated when the single physical connection is lost. The alarm is cleared when the single physical connection is restored.
- When MIIRedundancyEnable is enabled: the alarm is generated when both physical connections are lost. The alarm is cleared when one or both of the physical connections are restored.

8.3 NAT (Network Address Translation) Support

Network Address Translation (NAT) is a mechanism that maps a set of internal IP addresses used within a private network to global IP addresses, providing transparent routing to end hosts. The primary advantages of NAT include (1) Reduction in the number of global IP addresses required in a private network (global IP addresses are only used to connect to the Internet); (2) Better network security by hiding its internal architecture.

The following figure illustrates the gateway's supported NAT architecture.



The design of SIP creates a problem for VoIP traffic to pass through NAT. SIP uses IP addresses and port numbers in its message body and the NAT server can't modify SIP messages and therefore, can't change local to global addresses.

Two different streams traverse through NAT: signaling and media. A gateway (located behind a NAT) that initiates a signaling path has problems in receiving incoming signaling responses (they are blocked by the NAT server). Furthermore, the initiating gateway must notify the receiving gateway where to send the media.

To resolve these issues, the following mechanisms are available:

- STUN (refer to 'STUN' on page 425)
- First Incoming Packet Mechanism (refer to 'First Incoming Packet Mechanism' on page 426)
- RTP No-Op packets according to the avt-rtp-noop draft (refer to 'No-Op Packets' on page 426)

For information on SNMP NAT traversal, refer to the *SIP Series Reference Manual*.

8.3.1 STUN

Simple Traversal of UDP through NATs (STUN), based on RFC 3489 is a client / server protocol that solves most of the NAT traversal problems. The STUN server operates in the public Internet and the STUN clients are embedded in end-devices (located behind NAT). STUN is used both for the signaling and the media streams. STUN works with many existing NAT types and does not require any special behavior.

STUN enables the gateway to discover the presence (and types) of NATs and firewalls located between it and the public Internet. It provides the gateway with the capability to determine the public IP address and port allocated to it by the NAT. This information is later embedded in outgoing SIP / SDP messages and enables remote SIP user agents to reach the gateway. It also discovers the binding lifetime of the NAT (the refresh rate necessary to keep NAT 'Pinholes' open).

On startup, the gateway sends a STUN Binding Request. The information received in the STUN Binding Response (IP address:port) is used for SIP signaling. This information is updated every user-defined period (NATBindingDefaultTimeout).

At the beginning of each call and if STUN is required (i.e., not an internal NAT call), the media ports of the call are mapped. The call is delayed until the STUN Binding Response (that includes a global IP:port) for each media (RTP, RTCP and T.38) is received.

To enable STUN, perform the following:

- Enable the STUN feature using either the Embedded Web Server (refer to 'Configuring the Application Settings' on page 182) or the *ini* file (set EnableSTUN to 1).
- Define the STUN server address using one of the following methods:
 - Define the IP address of the primary and the secondary (optional) STUN servers using either the Embedded Web Server (refer to 'Configuring the Application Settings' on page 182) or the *ini* file (STUNServerPrimaryIP and STUNServerSecondaryIP). If the primary STUN server isn't available, the gateway attempts to communicate with the secondary server.
 - Define the domain name of the STUN server using the *ini* file parameter StunServerDomainName. The STUN client retrieves all STUN servers with an SRV query to resolve this domain name to an IP address and port, sort the server list, and use the servers according to the sorted list.
- Use the *ini* file parameter NATBindingDefaultTimeout to define the default NAT binding lifetime in seconds. STUN is used to refresh the binding information after this time expires.

**Notes:**

- STUN only applies to UDP (doesn't support TCP and TLS).
- STUN can't be used when the gateway is located behind a symmetric NAT.
- Use either the STUN server IP address (STUNServerPrimaryIP) or domain name (STUNServerDomainName) method, with priority to the first one.

8.3.2 First Incoming Packet Mechanism

If the remote gateway resides behind a NAT device, it's possible that the gateway can activate the RTP/RTCP/T.38 streams to an invalid IP address / UDP port. To avoid such cases, the gateway automatically compares the source address of the incoming RTP/RTCP/T.38 stream with the IP address and UDP port of the remote gateway. If the two are not identical, the transmitter modifies the sending address to correspond with the address of the incoming stream. The RTP, RTCP and T.38 can thus have independent destination IP addresses and UDP ports.

You can disable the NAT mechanism by setting the *ini* file parameter `DisableNAT` to 1. The two parameters `EnableIpAddrTranslation` and `EnableUdpPortTranslation` allow you to specify the type of compare operation that occurs on the first incoming packet. To compare only the IP address, set `EnableIpAddrTranslation` to 1, and `EnableUdpPortTranslation` to 0. In this case, if the first incoming packet arrives with only a difference in the UDP port, the sending addresses won't change. If both the IP address and UDP port need to be compared, then both parameters need to be set to 1.

8.3.3 No-Op Packets

The gateway's No-Op packet support can be used to verify Real-Time Transport Protocol (RTP) and T.38 connectivity, and to keep NAT bindings and Firewall pinholes open. The No-Op packets are available for sending in RTP and T.38 formats.

You can control the activation of No-Op packets by using the *ini* file parameter `NoOpEnable`. If No-Op packet transmission is activated, you can control the time interval in which No-Op packets are sent in the case of silence (i.e., no RTP or T.38 traffic). This is performed using the *ini* file parameter `NoOpInterval`. For a description of the RTP No-Op *ini* file parameters, refer to 'Networking Parameters' on page 299.

- **RTP No-Op:** The RTP No-Op support complies with IETF's draft-wing-avt-rtp-noop-03.txt (titled 'A No-Op Payload Format for RTP'). This IETF document defines a No-Op payload format for RTP. The draft defines the RTP payload type as dynamic. You can control the payload type with which the No-Op packets are sent. This is performed using the `RTPNoOpPayloadType` *ini* parameter (refer to 'Networking Parameters' on page 299). AudioCodes' default payload type is 120.
- **T.38 No-Op:** T.38 No-Op packets are sent only while a T.38 session is activated. Sent packets are a duplication of the previously sent frame (including duplication of the sequence number).



Note: Receipt of No-Op packets is always supported.

8.4 Point-to-Point Protocol over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) is a method of sending the Point-to-Point Protocol packets over an Ethernet network.

8.4.1 Point-to-Point Protocol (PPP) Overview

Point-to-Point Protocol (PPP) provides a method of transmitting data over serial point-to-point links. The protocol defines establishing, configuring and testing the data link connection and the network protocol.

The PPP standard describes a state machine used to establish a valid connection between two hosts over a serial connection. There are three major stages described, helping to establish a network layer (such as an IP) connection over the point-to-point link: LCP (Link Configuration Protocol) Authentication and NCP (Network Control Protocol). Once the network protocol is configured, the two hosts can communicate, sending network layer protocol (such as IP) over the PPP connection (a small PPP header is added at the beginning of each packet).

At the initial phase, the hosts use LCP (link configuration protocol) to negotiate for link characteristic and parameters. Packets sent in this phase have two octets of 'PPP header' followed by LCP message with variable length. Various parameters and options are negotiable at this phase, including MRU (maximum receive unit), Authentication Protocol, and others.

Once the link is established (each side sends a 'configure ack' message to the other side), the authentication phase may begin. The authentication phase is not mandatory. However, it is negotiated in the link configuration phase. A host may ask other hosts for authentication using Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The PAP sends the username and password to the remote host unencrypted.

The CHAP is a more sophisticated method of authentication. The two hosts share a 'secret'. The authenticator sends a 'challenge' to the host requesting authentication. The host performs a calculation (one-way hash) using the challenge received from the authenticator and the shared 'secret', and sends the result to the authenticator. The authenticator verifies the host if the result of the calculation is correct; otherwise it is rejected.

The last configuration phase, immediately after the authentication phase (or after the Link Configuration) is the Network Control Protocol. There is a family of control protocols for establishing and configuring different network-layer protocols, for example, IPCP (PPP Internet Protocol Control Protocol), IPv6CP (PPP IP v6 Control Protocol), and BCP (PPP Bridging Control Protocol). Each of them handles and manages the specific needs required by their respective network-layer protocol.

When working in an IP network, IPCP is used as the Network Configuration Protocol. The IPCP is used to configure the network layer of the hosts, requesting/declaring on IP Addresses.

Further information on PPP Protocol is available on the IETF Web site (<http://www.ietf.org/rfc/rfc1661.txt>). Further information on Password Authentication Protocol is available on the IETF Web site (<http://www.ietf.org/rfc/rfc1334.txt>). Further information on Challenge Handshake Authentication Protocol is available on the IETF Web site (<http://www.ietf.org/rfc/rfc1994.txt>). Further information on PPP Internet Protocol Control Protocol (IPCP) is available on the IETF Web site (<http://www.ietf.org/rfc/rfc1332.txt>).

8.4.2 PPPoE Overview

PPPoE is a method of sending the Point-to-Point Protocol over Ethernet network. PPPoE provides the ability to connect a network of hosts over a simple bridging access device to a remote Access Concentrator. Access control, billing and type of service can be done on a per-user, rather than a per-site, basis.

A common use of the PPPoE is in the ADSL market: The home PC is connected to a modem via Ethernet, and the PC uses the PPPoE to 'simulate' as if it was directly connected to the remote host on a point-to-point connection.

Since PPPoE frames are sent over Ethernet, each PPP session must learn the Ethernet address of the remote peer, as well as establish a unique session identifier. The PPPoE standard describes a discovery protocol that provides this. A PPPoE session begins with a discovery phase. Only after this discovery is completed can the PPP state machine start (with LCP, Authentication etc, as described above).

Each of the Ethernet frames carrying PPP session has a standard Ethernet header followed by PPPoE header, and is sent with the remote host Ethernet MAC address (except for the very first one, in the discovery phase, which is broadcasted to all hosts).

Further information on the transmission of PPPoE is available on the IETF website (<http://www.ietf.org/rfc/rfc2516.txt>).

8.4.3 PPPoE in AudioCodes Gateway

The AudioCodes gateway contains a PPPoE client embedded in its software. When configured, the gateway can try to connect to a remote PPPoE Access Concentrator.

When resetting the gateway after several BootP attempts and if PPPoE is enabled (see *ini* file parameter EnablePPPoE), the gateway tries to initiate a PPP session.

The gateway initiates a PPPoE discovery phase to discover a PPPoE Access Concentrator. It does this by broadcasting a discovery initialization packet (PADI). If an Access Concentrator exists and replies, the gateway tries to connect to this Access Concentrator. If this initial connection succeeds, then the PPP LCP phase starts - each side of the PPPoE connection sends an LCP configuration request to configure the PPP link. The gateway PPPoE client supports both PAP and CHAP authentications. The type of authentication protocol used is according to the request from the authentication server. In the LCP configuration phase, the server requires a specific authentication (none, PAP or CHAP are supported). The *ini* file parameters PPPoEUserName, PPPoEPassword, and PPPoEServerName are used to configure the authentication parameters. If the Access Concentrator is configured to operate in PAP, the PPPoEUserName and PPPoEPassword are used as Username and Password (in this case, the PPPoEServerName parameter is not used). If the Access Concentrator is configured to operate in CHAP, the PPPoEUserName parameter functions as Client Name (sent in the CHAP response packet), while the PPPoEPassword functions as the shared secret (calculated along with the challenge to produce the response). In this case, the PPPoEServerName is the name of the server (some hosts can be configured to authenticate to multiple servers. In such hosts, the server name is used to identify which secret should be used).

Note: The AudioCodes gateway, being a PPPoE client, requests no authentication.

After the gateway has been authenticated, it needs to configure a network layer protocol. The gateway uses the IP protocol. Therefore, the used NCP will be IPCP (IP Configuration Protocol). In this phase, if the *ini* file parameter PPPoEStaticIPAddress is defined, the gateway requests the remote host to assign this address for its use.

When working in a PPPoE environment, the gateway negotiates for its IP address (as described above). However, if you want to disable the PPPoE client, the gateway can be configured to use default values for IP address, subnet mask and default gateway. This can be done using *ini* file parameters PPPoERecoveryIPAddress, PPPoERecoverySubnetMask and PPPoERecoveryDfgwAddress. These parameters indicate to the gateway that if the PPPoE is disabled and no BootP server is activated, as required in the gateway to use a PPPoE environment, then the gateway should use these defaults for its IP configuration.

For a description of the *ini* file parameters for PPPoE, refer to 'Networking Parameters' on page 299.

8.5 IP Multicasting

The gateway supports IP Multicasting level 1 according to RFC 2236 (i.e., IGMP version 2) for RTP channels. The gateway is capable of transmitting and receiving Multicast packets.

8.6 Robust Reception of RTP Streams

This mechanism filters out unwanted RTP streams that are sent to the same port number on the gateway. These multiple RTP streams can result from traces of previous calls, call control errors, and deliberate attacks.

When more than one RTP stream reaches the gateway on the same port number, the gateway accepts only one of the RTP streams and rejects the rest of the streams. The RTP stream is selected according to the following procedure:

The first packet arriving on a newly opened channel sets the source IP address and UDP port from which further packets are received. Thus, the source IP address and UDP port identify the currently accepted stream. If a new packet arrives whose source IP address or UDP port are different to the currently accepted RTP stream, one of the following occurs:

- The gateway reverts to the new RTP stream when the new packet has a source IP address and UDP port that are the same as the remote IP address and UDP port that were stated during the opening of the channel.
- The packet is dropped when the new packet has any other source IP address and UDP port.

8.7 Multiple Routers Support

Multiple routers support is designed to assist the gateway when it operates in a multiple routers network. The gateway learns the network topology by responding to Internet Control Message Protocol (ICMP) redirections and caches them as routing rules (with expiration time).

When a set of routers operating within the same subnet serve as gateways to that network and intercommunicate using a dynamic routing protocol, the routers can determine the shortest path to a certain destination and signal the remote host the existence of the better route. Using multiple router support, the gateway can utilize these router messages to change its next hop and establish the best path.



Note: Multiple Routers support is an integral feature that doesn't require configuration.

8.8 Simple Network Time Protocol Support

The Simple Network Time Protocol (SNTP) client functionality generates requests and reacts to the resulting responses using the NTP version 3 protocol definitions (according to RFC 1305). Through these requests and responses, the NTP client synchronizes the system time to a time source within the network, thereby eliminating any potential issues should the local system clock 'drift' during operation. By synchronizing time to a network time source, traffic handling, maintenance, and debugging become simplified for the network administrator.

The NTP client follows a simple process in managing system time: the NTP client requests an NTP update, receives an NTP response, and updates the local system clock based on a configured NTP server within the network.

The client requests a time update from a specified NTP server at a specified update interval. In most situations, this update interval is every 24 hours based on when the system was restarted. The NTP server identity (as an IP address) and the update interval are user-defined that can be specified using the Embedded Web Server (refer to 'Configuring the Application Settings' on page 182), the *ini* file (NTPServerIP and NTPUpdateInterval respectively), or an SNMP MIB object (refer to the *SIP Series Reference Manual*).

When the client receives a response to its request from the identified NTP server it must be interpreted based on time zone, or location, offset that the system is to a standard point of reference called the Universal Time Coordinate (UTC). The time offset that the NTP client uses is configurable using the Embedded Web Server (refer to 'Configuring the Application Settings' on page 182), the *ini* file (NTPServerUTCOffset), or via an SNMP MIB object (refer to the *SIP Series Reference Manual*).

If required, the clock update is performed by the client as the final step of the update process. The update is performed in such a way as to be transparent to the end users. For instance, the response of the server may indicate that the clock is running too fast on the client. The client slowly robs bits from the clock counter to update the clock to the correct time. If the clock is running too slow, then in an effort to catch the clock up, bits are added to the counter, causing the clock to update quicker and catch up to the correct time. The advantage of this method is that it does not introduce any disparity in the system time that is noticeable to an end user or that could corrupt call timeouts and timestamps.

8.9 IP QoS via Differentiated Services (DiffServ)

DiffServ is an architecture providing different types or levels of service for IP traffic. DiffServ (according to RFC 2474) offers the capability to prioritize certain traffic types depending on their priority, thereby, accomplishing a higher-level QoS at the expense of other traffic types. By prioritizing packets, DiffServ routers can minimize transmission delays for time-sensitive packets such as VoIP packets.

The gateway can be configured to set a different DiffServ value to IP packets according to their class-of-service (i.e., Network, Premium Media, Premium Control, Gold, and Bronze).

For the mapping of an application to its class-of-service, refer to 'IEEE 802.1p/Q (VLANs and Priority)' on page 431.

The DiffServ parameters are described in 'Networking Parameters' on page 299.

8.10 VLANS and Multiple IPs

8.10.1 Multiple IPs

Media, Control, and Management (OAM) traffic in the gateway can be assigned one of the following IP addressing schemes:

- Single IP address for all traffic (i.e., Media, Control, and OAM).
- Separate IP address for each traffic type:

For separate IP addresses, the different traffic types are separated into three dedicated networks. Instead of a single IP address, the gateway is assigned three IP addresses and subnet masks, each relating to a different traffic type. This architecture enables you to integrate the gateway into a three-network environment that is focused on security and segregation. Each entity in the gateway (e.g., Web and RTP) is mapped to a single traffic type (according to the table in 'IEEE 802.1p/Q (VLANs and Priority)' on page 431) in which it operates.

- Dual IP mode (two separate IP addresses -- one for a specific traffic type and the other for a combination of two traffic types):

In Dual IP mode, the gateway is assigned two IP addresses for the different traffic types. One IP address is assigned with a combination of two traffic types (Media and Control, OAM and Control, or OAM and Media), while the other IP address is assigned to whichever traffic type not included in this combination. For example, a typical scenario using this mode would include one IP address assigned for Control and OAM, and another IP address assigned for Media.



Notes:

- A default Gateway is supported only for the Media traffic type; for the other two, use the IP Routing table.
- The IP address and subnet mask used in the Single IP Network mode are carried over to the OAM traffic type in the Multiple IP Network mode.

For detailed information on integrating the gateway into a VLAN and multiple IPs network, refer to 'Getting Started with VLANs and Multiple IPs' on page 434. For detailed information on configuring the multiple IP parameters, refer to 'Networking Parameters' on page 299.

8.10.2 IEEE 802.1p/Q (VLANs and Priority)

The Virtual Local Area Network (VLAN) mechanism enables the gateway to be integrated into a VLAN-aware environment that includes switches, routers and endpoints.

When in VLAN-enabled mode, each packet is tagged with values that specify its priority (class-of-service) (IEEE 802.1p) and the identifier (traffic type) of the VLAN to which it belongs (media, control, or management) (IEEE 802.1Q).

The class-of-service mechanism can be utilized to accomplish Ethernet QoS. Packets sent by the gateway to the Ethernet network are divided into five, different-priority classes (Network, Premium media, Premium control, Gold, and Bronze). The priority of each class is determined by a corresponding *ini* file parameter.

Traffic type tagging can be used to implement Layer 2 VLAN security. By discriminating traffic into separate and independent domains, the information is preserved within the VLAN. Incoming packets received from an incorrect VLAN are discarded.

Media traffic type is assigned 'Premium media' class of service, Management traffic type is assigned 'Bronze' class of service, and Control traffic type is assigned 'Premium control' class of service. For example, RTP/RTCP traffic is assigned the Media VLAN ID and 'Premium media' class of service, whereas Web traffic is assigned the Management VLAN ID and 'Bronze' class of service. Each of these parameters can be configured with a 802.1p/q value: traffic type to VLAN ID, and class of service to 802.1p priority.


Notes:

- As a safety measure, the VLAN mechanism is activated only when the gateway is loaded from the flash memory. Therefore, when using BootP:

Load an *ini* file with VlanMode set to 1 and SaveConfiguration set to 1. Then (after the gateway is active) reset the gateway with TFTP disabled or by using any method except for BootP.
- The gateway must be connected to a VLAN-aware switch, and the switch's PVID must be equal to the gateway's native VLAN ID.

For information on how to configure VLAN parameters, refer to 'Networking Parameters' on page [299](#).

For the mapping of an application to its class-of-service and traffic type, refer to the table below.

Table 8-1: Traffic / Network Types and Priority

| Application | Traffic / Network Types | Class-of-Service (Priority) |
|---------------------|--|--|
| Debugging interface | Management | Bronze |
| Telnet | Management | Bronze |
| DHCP | Management | Network |
| Web server (HTTP) | Management | Bronze |
| SNMP GET/SET | Management | Bronze |
| Web server (HTTPS) | Management | Bronze |
| IPSec IKE | Determined by the service | Determined by the service |
| RTP traffic | Media | Premium media |
| RTCP traffic | Media | Premium media |
| T.38 traffic | Media | Premium media |
| SIP | Control | Premium control |
| SIP over TLS (SIPS) | Control | Premium control |
| Syslog | Management | Bronze |
| ICMP | Management | Determined by the initiator of the request |
| ARP listener | Determined by the initiator of the request | Network |

Table 8-1: Traffic / Network Types and Priority

| Application | Traffic / Network Types | Class-of-Service (Priority) |
|-------------|--|--|
| SNMP Traps | Management | Bronze |
| DNS client | EnableDNSasOAM | Network |
| NTP | EnableNTPasOAM | Depends on the traffic type: Control: Premium control Management: Bronze |
| NFS | NFSServers_VlanType in the NFSServers table | Gold |

Operation:

- **Outgoing packets (from the gateway to the switch):**

All outgoing packets are tagged, each according to its interface (control, media or OAM). If the gateway's native ID is identical to one of the other IDs (usually to the OAM ID), this ID (e.g., OAM) is set to zero on outgoing packets (VlanSendNonTaggedOnNative set to 0). This method is called Priority Tagging (p tag without Q tag). If the parameter VlanSendNonTaggedOnNative is set to 1, the gateway sends regular packets (with no VLAN tag).

- **Incoming packets (from the switch to the gateway):**

The switch sends all packets intended for the gateway (according to the switch's configuration) to the gateway without altering them. For packets whose VLAN ID is identical to the switch's PVID. In this case, the switch removes the tag and sends a packet.

The gateway only accepts packets that have a VLAN ID identical to one of its interfaces (control, media or OAM). Packets with a VLAN ID that is 0 or packets without a tag are accepted only if the gateway's native VLAN ID is identical to the VLAN ID of one of its interfaces. In this case, the packets are sent to the relevant interface. All other packets are rejected.

8.10.3 Getting Started with VLANs and Multiple IPs

By default, the gateway operates without VLANs and multiple IPs, using a single IP address, subnet mask and default gateway IP address. This section provides an example of the configuration required to integrate the gateway into a VLAN and multiple IPs network using the Embedded Web Server (refer to 'Integrating Using the Embedded Web Server' on page 434) and *ini* file (refer to 'Integrating Using the ini File' on page 437).

The following table shows an example configuration that is used in the following sections.

Table 8-2: Example of VLAN and Multiple IPs Configuration

| Network Type | IP Address | Subnet Mask | Default Gateway IP Address | VLAN ID | External Routing Rule |
|--------------|--------------|-------------|----------------------------|---------|-----------------------|
| OAM | 10.31.174.50 | 255.255.0.0 | 0.0.0.0 | 4 | 83.4.87.X |
| Control | 10.32.174.50 | 255.255.0.0 | 0.0.0.0 | 5 | 130.33.4.6 |
| Media | 10.33.174.50 | 255.255.0.0 | 10.33.0.1 | 6 | -- |

Note that since a default gateway is available only for the Media network, for the gateway to be able to communicate with an external device / network on its OAM and Control networks, IP routing rules must be used.



Note: The values provided in 'Integrating Using the Embedded Web Server' on page 434 and 'Integrating Using the ini File' on page 437 are only used as an example and are to be replaced with actual values appropriate to your system.

8.10.3.1 Integrating Using the Embedded Web Server

The procedure below describes how to integrate the gateway into a VLAN and multiple IPs network using the Embedded Web Server.

➤ **To integrate the gateway into a VLAN and multiple IPs network using the Embedded Web Server, take these 7 steps:**

1. Access the Embedded Web Server (refer to 'Accessing the Embedded Web Server' on page 60).
2. Use the Software Upgrade Wizard ('Software Upgrade Wizard' on page 262) to load and *burn* the firmware version to the gateway (VLANs and multiple IPs support is available only when the firmware is burned to flash).

3. Configure the VLAN parameters by completing the following steps:
 - a. Open the 'VLAN Settings' screen (**Advanced Configuration** menu > **Network Settings** > **VLAN Settings** option).
 - b. Modify the VLAN parameters to correspond to the values shown in the following figure.

Figure 8-1: VLAN Settings Screen - Example

| VLAN Settings | |
|-----------------|--------|
| VLAN Mode | Enable |
| ID Settings | |
| Native VLAN ID | 4 |
| OAM VLAN ID | 4 |
| Control VLAN ID | 5 |
| Media VLAN ID | 6 |

- c. Click the **Submit** button to save your changes.
4. Configure the multiple IP parameters by completing the following steps:
 - a. Open the 'IP Settings' screen (**Advanced Configuration** menu > **Network Settings** > **IP Settings** option).
 - b. Modify the IP parameters to correspond to the values shown in the figure below. Note that the OAM, Control, and Media Network Settings parameters appear only after you select the options 'Multiple IP Networks' or 'Dual IP' in the field 'IP Networking Mode'.



Note: Configure the OAM parameters only if the OAM networking parameters are different from the networking parameters used in the Single IP Network mode.

Figure 8-2: IP Settings Screen - Example

| IP Settings | |
|---------------------------------|----------------------|
| IP Networking Mode | Multiple IP Networks |
| OAM Network Settings | |
| IP Address | 10.31.174.50 |
| Subnet Mask | 255.255.0.0 |
| Default Gateway Address | 0.0.0.0 |
| Control Network Settings | |
| IP Address | 10.32.174.50 |
| Subnet Mask | 255.255.0.0 |
| Default Gateway Address | 0.0.0.0 |
| Media Network Settings | |
| IP Address | 10.33.174.50 |
| Subnet Mask | 255.255.0.0 |
| Default Gateway Address | 10.33.0.1 |

- c. Click the **Submit** button to save your changes.
5. Configure the IP Routing table by completing the following steps (the IP Routing table is required to define static routing rules for the OAM and Control networks since a default gateway isn't supported for these networks):
 - a. Open the 'IP Routing Table' screen (**Advanced Configuration** menu > **Network Settings** > **IP Routing Table** option).

Figure 8-3: IP Routing Table - Example

| Routing Table | | | | | | | |
|----------------------------|------------------------|------------------|--------------------|------------|-----------|-----------|--|
| Delete Row | Destination IP Address | Destination Mask | Gateway IP Address | TTL | Hop Count | Interface | |
| 1 <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | 10.33.0.1 | 2147483647 | 1 | Media | |
| 2 <input type="checkbox"/> | 10.31.0.0 | 255.255.0.0 | 10.31.174.50 | 2147483647 | 0 | OAM | |
| 3 <input type="checkbox"/> | 10.32.0.0 | 255.255.0.0 | 10.32.174.50 | 2147483647 | 0 | Control | |
| 4 <input type="checkbox"/> | 10.33.0.0 | 255.255.0.0 | 10.33.174.50 | 2147483647 | 0 | Media | |
| 5 <input type="checkbox"/> | 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 2147483647 | 1 | OAM | |
| 6 <input type="checkbox"/> | 127.0.0.1 | 255.255.255.255 | 127.0.0.1 | 2147483647 | 0 | OAM | |

- b. Use the 'Add a new table entry' pane to add the routing rules shown in the following table:

| Destination IP Address | Destination Mask | Gateway IP Address | Hop Count | Network Type |
|------------------------|------------------|--------------------|-----------|--------------|
| 130.33.4.6 | 255.255.255.255 | 10.32.0.1 | 20 | Control |
| 83.4.87.6 | 255.255.255.0 | 10.31.0.1 | 20 | OAM |

- a. Click the **Submit** button to save your changes.
6. Save your changes to flash memory (refer to 'Saving Configuration' on page 278).
7. Reset the gateway (refer to 'Resetting the Gateway' on page 279).

8.10.3.2 Integrating Using the ini File

The procedure below describes how to integrate the gateway into a VLAN and multiple IPs network using the *ini* file.

➤ **To integrate the gateway into a VLAN and multiple IPs network using the *ini* file, take these 3 steps:**

1. Prepare an *ini* file with relevant parameters. Refer to the following notes:
 - If the BootP/TFTP utility and the OAM interface are located in the same network, the Native VLAN ID (VlanNativeVlanId) must be equal to the OAM VLAN ID (VlanOamVlanId), which in turn must be equal to the PVID of the switch port to which the gateway is connected. Therefore, set the PVID of the switch port to 4 (in this example).
 - Configure the OAM parameters (LocalOAMPAAddress, LocalOAMSubnetMask and LocalOAMDefaultGW) only if the OAM networking parameters are different from the networking parameters used in the Single IP Network mode.
 - The IP Routing table is required to define static routing rules for the OAM and Control networks since a default gateway isn't supported for these networks.

Below is an example of an *ini* file containing VLAN and Multiple IPs parameters:

```
; VLAN Configuration
VlanMode=1
VlanOamVlanId=4
VlanNativeVlanId=4
VlanControlVlanId=5
VlanMediaVlanID=6
; Multiple IPs Configuration
EnableMultipleIPs=1
LocalMediaIPAddress=10.33.174.50
LocalMediaSubnetMask=255.255.0.0
LocalMediaDefaultGW=10.33.0.1
LocalControlIPAddress=10.32.174.50
LocalControlSubnetMask=255.255.0.0
LocalControlDefaultGW=0.0.0.0
LocalOAMPAAddress=10.31.174.50
LocalOAMSubnetMask=255.255.0.0
LocalOAMDefaultGW=0.0.0.0
; IP Routing table parameters
RoutingTableDestinationsColumn = 130.33.4.6, 83.4.87.6
RoutingTableDestinationMasksColumn = 255.255.255.255 ,
255.255.255.0
RoutingTableGatewaysColumn = 10.32.0.1 , 10.31.0.1
RoutingTableInterfacesColumn = 1 , 0
RoutingTableHopsCountColumn = 20,20
```

2. Use the BootP/TFTP utility (refer to the *SIP Series Reference Manual*) to load and *burn* (-fb option) the firmware version and the *ini* file you prepared in the previous step to the gateway (VLANs and multiple IPs support is available only when the firmware is burned to flash).
3. Reset the gateway after disabling it on the BootP/TFTP utility.

9 Advanced PSTN Configuration

9.1 Clock Settings

The gateway Clock Settings can be configured to generate its own timing signals, use an internal clock, or recover them from one of the E1/T1 trunks.

➤ **To use the internal gateway clock source, configure the following parameters:**

- TDMBusClockSource = 1
- ClockMaster = 1 (for all gateway trunks)

➤ **To use the recovered clock option configure the following parameters:**

- TDMBusClockSource = 4
- ClockMaster_x = 0 (for all 'slave' gateway trunks connected to PBX#1)
- ClockMaster_x = 1 (for all 'master' gateway trunks connected to PBX#2)

The above assumes that the gateway recovers its internal clock from one of the 'slave' trunks connected to PBX#1 and provides clock to PBX#2 on its 'master' trunks.

In addition, it's necessary to define from which of the 'slave' trunks the gateway recovers its clock:

- TDMBusPSTNAutoClockEnable = 1 (The gateway automatically selects one of the connected 'slave' trunks)
- Or -
- TDMBusLocalReference = # (Trunk index: 0 to 3, default = 0)



Notes:

- To configure the TDM Bus Clock Source parameters using the Embedded Web Server, refer to 'Configuring the TDM Bus Settings' on page [221](#).
- When the gateway is used in a 'non-span' configuration, the internal gateway clock must be used (as explained above).

9.2 Release Reason Mapping

This appendix describes the available mapping mechanisms of SIP Responses to Q.850 Release Causes and vice versa.

The existing mapping of ISDN Release Causes to SIP Responses is described in 'Fixed Mapping of ISDN Release Reason to SIP Response' on page 441 and 'Fixed Mapping of SIP Response to ISDN Release Reason' on page 443. To override this hard-coded mapping and flexibly map SIP Responses to ISDN Release Causes, use the *ini* file (CauseMapISDN2SIP and CauseMapSIP2ISDN, as described in 'ISDN and CAS Interworking-Related Parameters' on page 343) or the Embedded Web Server (refer to 'Release Cause Mapping' on page 144).

It is also possible to map the less commonly-used SIP Responses to a single default ISDN Release Cause. Use the parameter DefaultCauseMapISDN2IP (described in 'ISDN and CAS Interworking-Related Parameters' on page 343) to define a default ISDN Cause that is always used except when the following Release Causes are received: Normal Call Clearing (16), User Busy (17), No User Responding (18) or No Answer from User (19). This mechanism is only available for Tel-to-IP calls.

9.2.1 Reason Header

The gateway supports the Reason header according to RFC 3326. The Reason header is used to convey information describing the disconnection cause of a call:

- **Sending Reason header:** If a call is disconnected from the Tel side (ISDN), the Reason header is set to the received Q.850 cause in the appropriate message (BYE / CANCEL / final failure response) and sent to the SIP side. If the call is disconnected because of a SIP reason, the Reason header is set to the appropriate SIP response.
- **Receiving Reason header:** If a call is disconnected from the IP side and the SIP message includes the Reason header, it is sent to the Tel side according to the following logic:
 - If the Reason header includes a Q.850 cause, it is sent as is.
 - If the Reason header includes a SIP response:
 - ◆ If the message is a final response, the response status code is translated to Q.850 format and passed to ISDN.
 - ◆ If the message isn't a final response, it is translated to a Q.850 cause.
 - When the Reason header is received twice (i.e., SIP Reason and Q.850), the Q.850 takes precedence over the SIP reason and is sent to the Tel side.

9.2.2 Fixed Mapping of ISDN Release Reason to SIP Response

The following table describes the mapping of ISDN release reason to SIP response.

Table 9-1: Mapping of ISDN Release Reason to SIP Response

| ISDN Release Reason | Description | SIP Response | Description |
|---------------------|--|--------------|-------------------------|
| 1 | Unallocated number | 404 | Not found |
| 2 | No route to network | 404 | Not found |
| 3 | No route to destination | 404 | Not found |
| 6 | Channel unacceptable | 406* | Not acceptable |
| 7 | Call awarded and being delivered in an established channel | 500 | Server internal error |
| 16 | Normal call clearing | _* | BYE |
| 17 | User busy | 486 | Busy here |
| 18 | No user responding | 408 | Request timeout |
| 19 | No answer from the user | 480 | Temporarily unavailable |
| 21 | Call rejected | 403 | Forbidden |
| 22 | Number changed w/o diagnostic | 410 | Gone |
| 26 | Non-selected user clearing | 404 | Not found |
| 27 | Destination out of order | 502 | Bad gateway |
| 28 | Address incomplete | 484 | Address incomplete |
| 29 | Facility rejected | 501 | Not implemented |
| 30 | Response to status enquiry | 501* | Not implemented |
| 31 | Normal unspecified | 480 | Temporarily unavailable |
| 34 | No circuit available | 503 | Service unavailable |
| 38 | Network out of order | 503 | Service unavailable |
| 41 | Temporary failure | 503 | Service unavailable |
| 42 | Switching equipment congestion | 503 | Service unavailable |
| 43 | Access information discarded | 502* | Bad gateway |
| 44 | Requested channel not available | 503* | Service unavailable |
| 47 | Resource unavailable | 503 | Service unavailable |
| 49 | QoS unavailable | 503* | Service unavailable |
| 50 | Facility not subscribed | 503* | Service unavailable |
| 55 | Incoming calls barred within CUG | 403 | Forbidden |
| 57 | Bearer capability not authorized | 403 | Forbidden |
| 58 | Bearer capability not presently available | 503 | Service unavailable |

Table 9-1: Mapping of ISDN Release Reason to SIP Response

| ISDN Release Reason | Description | SIP Response | Description |
|---------------------|--|--------------|---------------------------|
| 63 | Service/option not available | 503* | Service unavailable |
| 65 | Bearer capability not implemented | 501 | Not implemented |
| 66 | Channel type not implemented | 480* | Temporarily unavailable |
| 69 | Requested facility not implemented | 503* | Service unavailable |
| 70 | Only restricted digital information bearer capability is available | 503* | Service unavailable |
| 79 | Service or option not implemented | 501 | Not implemented |
| 81 | Invalid call reference value | 502* | Bad gateway |
| 82 | Identified channel does not exist | 502* | Bad gateway |
| 83 | Suspended call exists, but this call identity does not | 503* | Service unavailable |
| 84 | Call identity in use | 503* | Service unavailable |
| 85 | No call suspended | 503* | Service unavailable |
| 86 | Call having the requested call identity has been cleared | 408* | Request timeout |
| 87 | User not member of CUG | 503 | Service unavailable |
| 88 | Incompatible destination | 503 | Service unavailable |
| 91 | Invalid transit network selection | 502* | Bad gateway |
| 95 | Invalid message | 503 | Service unavailable |
| 96 | Mandatory information element is missing | 409* | Conflict |
| 97 | Message type non-existent or not implemented | 480* | Temporarily not available |
| 98 | Message not compatible with call state or message type non-existent or not implemented | 409* | Conflict |
| 99 | Information element non-existent or not implemented | 480* | Not found |
| 100 | Invalid information elements contents | 501* | Not implemented |
| 101 | Message not compatible with call state | 503* | Service unavailable |
| 102 | Recovery of timer expiry | 408 | Request timeout |
| 111 | Protocol error | 500 | Server internal error |
| 127 | Interworking unspecified | 500 | Server internal error |

* Messages and responses were created as the 'ISUP to SIP Mapping' draft doesn't specify their cause code mapping.

9.2.3 Fixed Mapping of SIP Response to ISDN Release Reason

The following table describes the mapping of SIP response to ISDN release reason.

Table 9-2: Mapping of SIP Response to ISDN Release Reason

| SIP Response | Description | ISDN Release Reason | Description |
|--------------|------------------------------------|---------------------|--------------------------------|
| 400* | Bad request | 31 | Normal, unspecified |
| 401 | Unauthorized | 21 | Call rejected |
| 402 | Payment required | 21 | Call rejected |
| 403 | Forbidden | 21 | Call rejected |
| 404 | Not found | 1 | Unallocated number |
| 405 | Method not allowed | 63 | Service/option unavailable |
| 406 | Not acceptable | 79 | Service/option not implemented |
| 407 | Proxy authentication required | 21 | Call rejected |
| 408 | Request timeout | 102 | Recovery on timer expiry |
| 409 | Conflict | 41 | Temporary failure |
| 410 | Gone | 22 | Number changed w/o diagnostic |
| 411 | Length required | 127 | Interworking |
| 413 | Request entity too long | 127 | Interworking |
| 414 | Request URI too long | 127 | Interworking |
| 415 | Unsupported media type | 79 | Service/option not implemented |
| 420 | Bad extension | 127 | Interworking |
| 480 | Temporarily unavailable | 18 | No user responding |
| 481* | Call leg/transaction doesn't exist | 127 | Interworking |
| 482* | Loop detected | 127 | Interworking |
| 483 | Too many hops | 127 | Interworking |
| 484 | Address incomplete | 28 | Invalid number format |
| 485 | Ambiguous | 1 | Unallocated number |
| 486 | Busy here | 17 | User busy |
| 488 | Not acceptable here | 31 | Normal, unspecified |
| 500 | Server internal error | 41 | Temporary failure |
| 501 | Not implemented | 38 | Network out of order |
| 502 | Bad gateway | 38 | Network out of order |
| 503 | Service unavailable | 41 | Temporary failure |
| 504 | Server timeout | 102 | Recovery on timer expiry |

Table 9-2: Mapping of SIP Response to ISDN Release Reason

| SIP Response | Description | ISDN Release Reason | Description |
|--------------|-------------------------|---------------------|----------------------|
| 505* | Version not supported | 127 | Interworking |
| 600 | Busy everywhere | 17 | User busy |
| 603 | Decline | 21 | Call rejected |
| 604 | Does not exist anywhere | 1 | Unallocated number |
| 606* | Not acceptable | 38 | Network out of order |

* Messages and responses were created as the 'ISUP to SIP Mapping' draft doesn't specify their cause code mapping.

9.3 ISDN Overlap Dialing

Overlap dialing is a dialing scheme used by several ISDN variants to send and / or receive called number digits one after the other (or several at a time). This is as opposed to en-bloc dialing in which a complete number is sent.

The gateway can optionally support ISDN overlap dialing for incoming ISDN calls for the entire gateway by setting the *ini* file parameter `ISDNRxOverlap` to 1, or per E1/T1 span by setting `ISDNRxOverlap_x` to 1 (where *x* represents the number of the trunk -- 0 to 3). For configuring ISDN overlap dialing using the Embedded Web Server, refer to 'Trunk Settings' on page 206.

To play a Dial tone to the ISDN user side when an empty called number is received, set `ISDNINCallsBehavior` = 65536 (bit #16). This results in the Progress Indicator to be included in the SetupAck ISDN message.

The gateway stops collecting digits (for ISDN-to-IP calls) when:

- The sending device transmits a 'sending complete' IE in the ISDN Setup or the following INFO messages to signal that no more digits are going to be sent.
- The inter-digit timeout (configured by the parameter `TimeBetweenDigits`) expires. The default for this timeout is 4 seconds.
- The maximum allowed number of digits (configured by the parameter `MaxDigits`) is reached. The default is 30 digits.
- A match is found with the defined digit map (configured by the parameter, `DigitMapping`).

Relevant parameters (described in 'PSTN Parameters' on page 340):

- `ISDNRxOverlap`
- `ISDNRxOverlap_x`
- `TimeBetweenDigits`
- `MaxDigits`
- `ISDNINCallsBehavior`
- `DigitMapping`

9.4 Using ISDN NFAS

In regular (non-NFAS) T1 ISDN trunks, a single 64 kbps channel carries signaling for the other 23 B-channels of that particular T1 trunk. This channel is called the D-channel and usually resides on timeslot # 24.

The ISDN Non-Facility Associated Signaling (NFAS) feature enables use of a single D-channel to control multiple PRI interfaces.

With NFAS it is possible to define a group of T1 trunks, called an NFAS group, in which a single D-channel carries ISDN signaling messages for the entire group. The NFAS group's B-channels are used to carry traffic, such as voice or data. The NFAS mechanism also enables definition of a backup D-channel on a different T1 trunk, to be used if the primary D-channel fails.

The NFAS group comprises several T1 trunks. Each T1 trunk is called an 'NFAS member'. The T1 trunk whose D-channel is used for signaling is called the 'Primary NFAS Trunk'. The T1 trunk whose D-channel is used for backup signaling is called the 'Backup NFAS Trunk'. The primary and backup trunks each carry 23 B-channels while all other NFAS trunks each carry 24 B-channels.

The gateway supports multiple NFAS groups. Each group should contain different T1 trunks.

The NFAS group is identified by an NFAS GroupID number (possible values are 1, 2, 3 and 4). To assign a number of T1 trunks to the same NFAS group, use the *ini* file parameter `NFASGroupNumber_x = groupID` (where *x* is the physical trunkID -- 0 to 3) or the Embedded Web Server (refer to 'Trunk Settings' on page 206).

The parameter '`DchConfig_x = Trunk_type`' is used to define the type of NFAS trunk. `Trunk_type` is set to 0 for the primary trunk, to 1 for the backup trunk, and to 2 for an ordinary NFAS trunk. '*x*' depicts the physical trunkID (0 to 3). You can also use the Embedded Web Server (refer to 'Trunk Settings' on page 206).

For example, to assign the first four gateway T1 trunks to NFAS group #1, in which trunk #0 is the primary trunk and trunk #1 is the backup trunk, use the following configuration:

```
NFASGroupNumber 0 = 1
NFASGroupNumber 1 = 1
NFASGroupNumber 2 = 1
NFASGroupNumber 3 = 1
DchConfig 0 = 0           ;Primary T1 trunk
DchConfig 1 = 1           ;Backup T1 trunk
DchConfig 2 = 2           ;24 B-channel NFAS trunk
DchConfig 3 = 2           ;24 B-channel NFAS trunk
```

The NFAS parameters are described in 'PSTN Parameters' on page 340.

9.4.1 NFAS Interface ID

Several ISDN switches require an additional configuration parameter per T1 trunk that is called 'Interface Identifier'. In NFAS T1 trunks, the Interface Identifier is sent explicitly in Q.931 Setup / Channel Identification IE for all NFAS trunks, except for the B-channels of the Primary trunk (refer to note below).

The Interface ID can be defined per each member (T1 trunk) of the NFAS group, and must be coordinated with the configuration of the Switch. The default value of the Interface ID is identical to the number of the physical T1 trunk (0 for the first gateway trunk, 1 for the second gateway T1 trunk, and so on, up to 3).

To define an explicit Interface ID for a T1 trunk (that is different from the default), use the following parameters:

- ISDNIBehavior_x = 512 (x = 0 to 3 identifying the gateway physical trunk)
- ISDNNFASInterfaceID_x = ID (x = 0 to 255)



Notes:

- Usually the Interface Identifier is included in the Q.931 Setup/Channel Identification IE only on T1 trunks that doesn't contain the D-channel. Calls initiated on B-channels of the Primary T1 trunk, by default, don't contain the Interface Identifier. Setting the parameter ISDNIBehavior_x to 2048' forces the inclusion of the Channel Identifier parameter also for the Primary trunk.
- The parameter ISDNNFASInterfaceID_x = ID can define the 'Interface ID' for any Primary T1 trunk, even if the T1 trunk is not a part of an NFAS group. However, to include the Interface Identifier in Q.931 Setup/Channel Identification IE configure ISDNIBehavior_x = 2048 in the *ini* file.

9.4.2 Working with DMS-100 Switches

The DMS-100 switch requires the following NFAS Interface ID definitions:

- InterfaceID #0 for the Primary trunk
- InterfaceID #1 for the Backup trunk
- InterfaceID #2 for a 24 B-channel T1 trunk
- InterfaceID #3 for a 24 B-channel T1 trunk
- Etc.

For example, if four T1 trunks on a gateway are configured as a single NFAS group with Primary and Backup T1 trunks that is used with a DMS-100 switch, the following parameters should be used:

```
NFASGroupNumber 0 = 1
NFASGroupNumber 1 = 1
NFASGroupNumber 2 = 1
NFASGroupNumber 3 = 1
DchConfig 0 = 0      ;Primary T1 trunk
DchConfig 1 = 1      ;Backup T1 trunk
DchConfig 2 = 2      ;B-Channel NFAS trunk
DchConfig 3 = 2      ;B-channel NFAS trunk
```

If there is no NFAS Backup trunk, the following configuration should be used:

```
ISDNNFASInterfaceID 0 = 0
ISDNNFASInterfaceID 1 = 2
ISDNNFASInterfaceID 2 = 3
ISDNNFASInterfaceID 3 = 4
ISDNBehavior = 512 ;This parameter should be added because of
;ISDNNFASInterfaceID configuration above
NFASGroupNumber 0 = 1
NFASGroupNumber 1 = 1
NFASGroupNumber 2 = 1
NFASGroupNumber_3 = 1
DchConfig 0 = 0 ;Primary T1 trunk
DchConfig 1 = 2 ;B-Channel NFAS trunk
DchConfig 2 = 2 ;B-Channel NFAS trunk
DchConfig 3 = 2 ;B-channel NFAS trunk
```

9.4.3 Creating an NFAS-Related Trunk Configuration On-The-Fly

The procedures for creating and deleting an NFAS group on-the-fly must be performed in the correct order, as described below.

➤ **To create an NFAS Group, take these 3 steps:**

1. If there's a backup ('secondary') trunk for this group, it must be configured first.
2. Configure the primary trunk before configuring any NFAS ('slave') trunk.
3. Configure NFAS ('slave') trunks.

➤ **To stop / delete an NFAS Group, take these 3 steps:**

1. Stop / delete all NFAS ('slave') trunks.
2. Stop / delete the backup trunk if a backup trunk exists.
3. Stop / delete the primary trunk.



Notes:

- All trunks in the group must be configured with the same values for trunk parameters TerminationSide, ProtocolType, FramingMethod, and LineCode.
- After stopping or deleting the backup trunk, delete the group and then reconfigure it.

9.5 Redirect Number and Calling Name (Display)

The following tables define the gateway redirect number and calling name (Display) support for various PRI variants:

Table 9-3: Calling Name (Display)

| | DMS-100 | NI-2 | 4/5ESS | Euro ISDN |
|--------------|----------------|-------------|---------------|------------------|
| NT→TE | Yes | Yes | No | Yes |
| TE→NT | Yes | Yes | No | No |

Table 9-4: Redirect Number

| | DMS-100 | NI-2 | 4/5ESS | Euro ISDN |
|--------------|----------------|-------------|---------------|------------------|
| NT→TE | Yes | Yes | Yes | Yes |
| TE→NT | Yes | Yes | Yes | No |

10 Media Server Capabilities

This section provides information on the Mediant 1000's media server capabilities:

- Multi-party conferencing (refer to 'Conference Server' on page 449)
- Announcements playing and recording (refer to 'Announcement Server' on page 463)
- IP-to-IP Transcoding (refer to 'IP-to-IP Transcoding' on page 474)

The Mediant 1000 conference, transcoding, announcement and media server applications can be used separately, each on a different platform, or all on the same gateway. The SIP URI name in the INVITE message is used to identify the resource (media server, conference or announcement) to which the SIP session is addressed.

The number of DSP channels that are allocated for IP conferences, transcoding and IP announcements is determined by the parameter MediaChannels. Other DSP channels can be used for PSTN media server.

The Mediant 1000 SIP implementation is based on the decomposition model described in the following IETF drafts:

- 'A Multi-party Application Framework for SIP' (draft-ietf-sipping-cc-framework-06.txt)
- 'Models for Multi Party Conferencing in SIP' (draft-ietf-sipping-conferencing-framework-05.txt)
- 'A Framework for Conferencing with the Session Initiation Protocol (SIP)' (RFC 4353)
- 'Basic Network Media Services with SIP' (RFC 4240)
- 'Media Server Control Markup Language (MSCML) and Protocol' (draft-vandyke-mscml-06.txt)



Note: To use the Mediant 1000's advanced Announcement capabilities, it's essential that the *ini* file parameter AMSProfile be set to 1.

10.1 Conference Server

The Mediant 1000 supports dial-in, multi-party conferencing. In conference applications, the Mediant 1000 functions as a centralized conference bridge. In ad-hoc or prearranged conferences, users 'invite' the conference bridge. The conference bridge mixes the media and sends it to all participants.

The Mediant 1000 supports the following interfaces for conferencing:

- Simple (according to NetAnn) -- refer to 'Simple Conferencing (NetAnn)' on page 450
- Advanced (according to MSCML) -- refer to 'Advanced Conferencing (MSCML)' on page 452

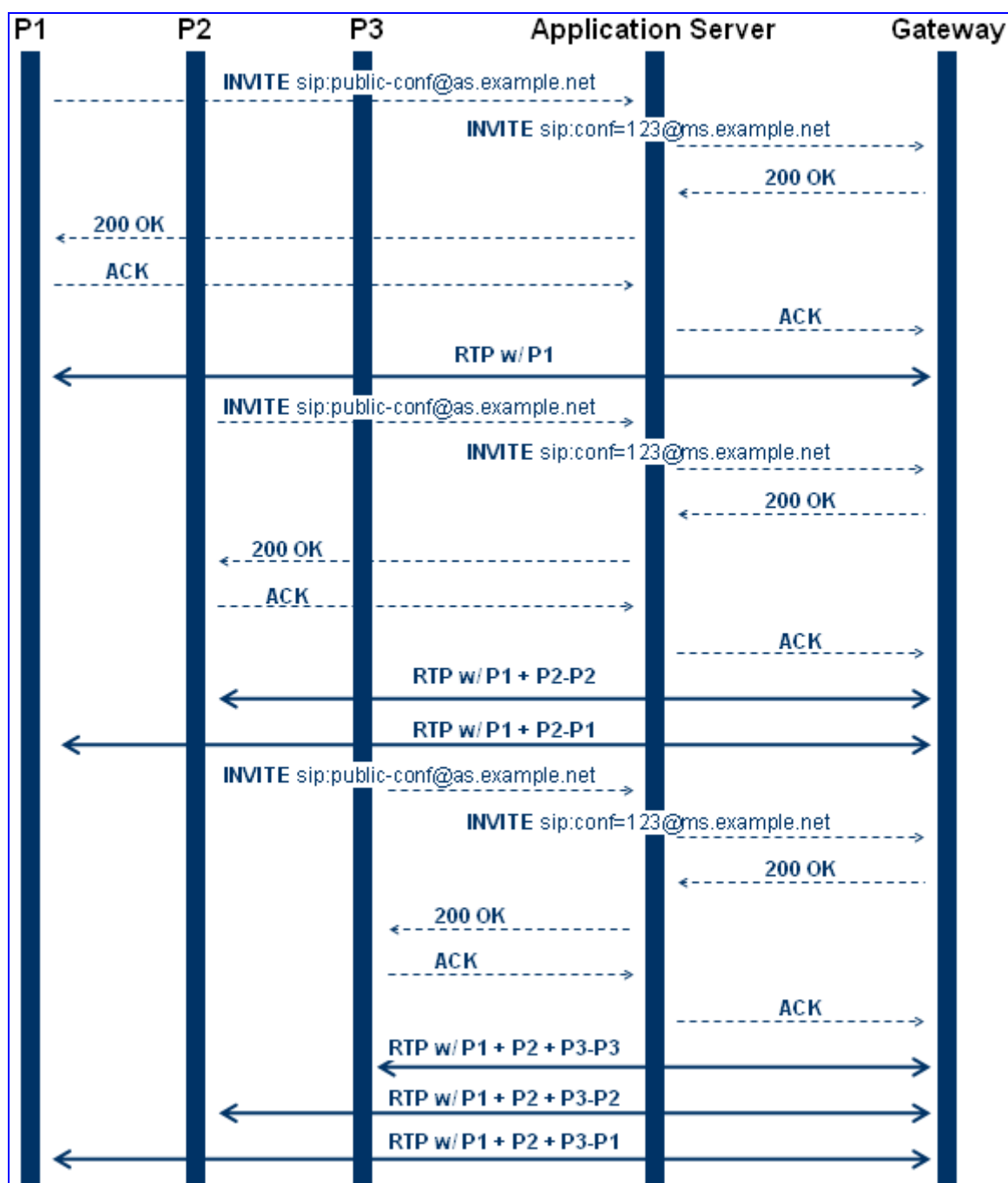


Note: The conference application is a special order option.

10.1.1 Simple Conferencing (NetAnn)

10.1.1.1 SIP Call Flow

Figure 10-1: Simple Conferencing SIP Call Flow



10.1.1.2 Creating a Conference

The gateway creates a conference call when the first user joins the conference. To create a conference, the Application Server should send a regular SIP INVITE message to the gateway. The User Part of that Request-URI should include both the Conference Service Identifier (indicating that the requested Media Service is a Conference) and a Unique Conference Identifier (identifying a specific instance of a conference).

```
INVITE sip: conf100@audiocodes.com SIP/2.0
```

By default, a request to create a conference reserves three resources on the gateway. It is possible to reserve a larger number of resources in advance by adding the number of required participants to the User Part of the Request-URI. For example, '6conf100' reserves six resources for the duration of the conference. If the gateway can allocate the requested number of resources, it responds with a 200 OK.

The Conference Service Identifier can be set using the *ini* file (ConferenceID) or Embedded Web Server (refer to 'Supplementary Services' on page 113). By default, it is set to 'conf'.

10.1.1.3 Joining a Conference

To join an existing conference, the Application Server sends a SIP INVITE message with the same Request-URI as the one that created the conference. Each conference participant can use a different coder, negotiated with the gateway using usual SIP negotiation.

If more than the initially requested number of participants try to join the conference (i.e., four resources were reserved and a fifth INVITE is received) and the gateway has an available resource, that request shall be granted.

If an INVITE to join an existing conference is received with a request to reserve a larger number of participants than initially requested, it shall be granted if the gateway has available resources. A request for a smaller number of participants shall not be granted as this might create a situation where existing legs would need to be disconnected.

The maximal number of participants in a single conference is 60. The maximal number of participants that actually participate in the mix at a given time is 3 (the loudest legs).

The Application Server can place a participant on Hold/Un-hold by sending the appropriate SIP Re-INVITE on that participant dialog.

10.1.1.4 Terminating a Conference

The gateway never disconnects an existing conference leg. If a BYE is received on an existing leg, it is disconnected, but the resource is still saved if the same leg (or a different one) wants to re-join the conference. This logic occurs only for the initial number of reserved legs.

For example:

1. INVITE reserves three legs.
2. A, B, and C join the conference.
3. A disconnects.
4. A joins (guaranteed).

5. D joins.
6. A disconnects.
7. A joins (not guaranteed).

Sending a BYE request to the gateway terminates the participant's SIP session and removes it from the conference. The final BYE from the last participant ends the conference and releases all conference resources.

10.1.1.5 PSTN Participants

Adding PSTN participants is done by performing loopback from the IP side (TEL2IP have the Mediant 1000 IP address).

If the destination phone number in the incoming call from the PSTN is equal to the Conference Service Identifier and Unique Conference Identifier, the participant joins the conference.

A PSTN participant uses two DSP channels (caused by the IP loopback).

10.1.2 Advanced Conferencing (MSCML)

10.1.2.1 Creating a Conference

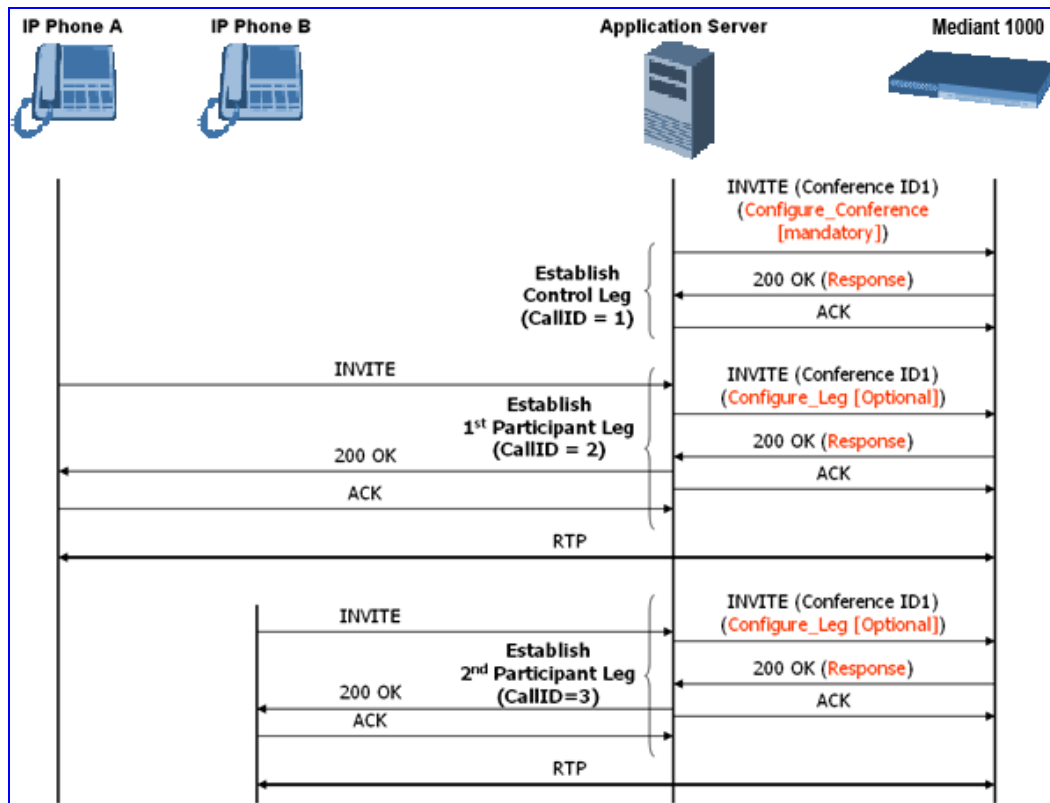
The gateway creates a conference call when the first INVITE is received from the Application Server (same as NetAnn). The Unique Conference Identifier is used to join participants to the same conference. This first INVITE must include a `<configure_conference>` MSCML request body. If this body is not included, a simple conference is established. This first leg is the Control Leg, which is different from a regular Participant Leg. The Control Leg is used to perform operations for the whole conference.

The MSCML response to the first INVITE is sent in the 200 OK SIP response. If no error occurs, the response is: `<response request="configure_conference" code="200" text="OK"/>`.

The `<configure_conference>` can include the following attributes:

- **Id:** identification number of the MSCML request. This is used to correlate between MSCML requests and responses.
- **Reservedtalkers:** defines the maximum number of talker legs. As the gateway does not support "listener only" legs, this actually sets the maximum number of participants in the conference. The gateway reserves this number of participants for the entire duration of the conference. If a participant leg decides to leave the conference by issuing a BYE, the resource is not freed, thereby allowing that same leg (or a new one) to join at any stage.
- **Reserveconfmedia:** determines if Media Services such as Play or Record can be applied to the conference. If set to Yes, the gateway reserves the necessary amount of resources to play an announcement to the whole conference or record the whole conference. The Application Server can change the value of reserveconfmedia during an existing conference. By default, reserveconfmedia is set to Yes.

Figure 10-2: Advanced Conferencing SIP Call Flow



10.1.2.2 Joining a Conference

To join an existing conference, the Application Server sends a SIP INVITE message with the same Request-URI as the one that created the conference. The INVITE message may include a <configure_leg> MSCML request body. If not included, defaults are used for that leg attributes.

The <configure_leg> can include the following attributes:

- **Id:** identification number of the MSCML request. This is used to correlate between MSCML requests and responses.
- **Type:** Talker / Listener. If set to Listener, the incoming RTP from that leg does not participate in the conference mix. The default is Talker.
- **Mixmode:**
 - Full: RTP from this leg participates in the mix (default).
 - Mute: RTP from this leg is not participating in the mix.

10.1.2.3 Modifying a Conference

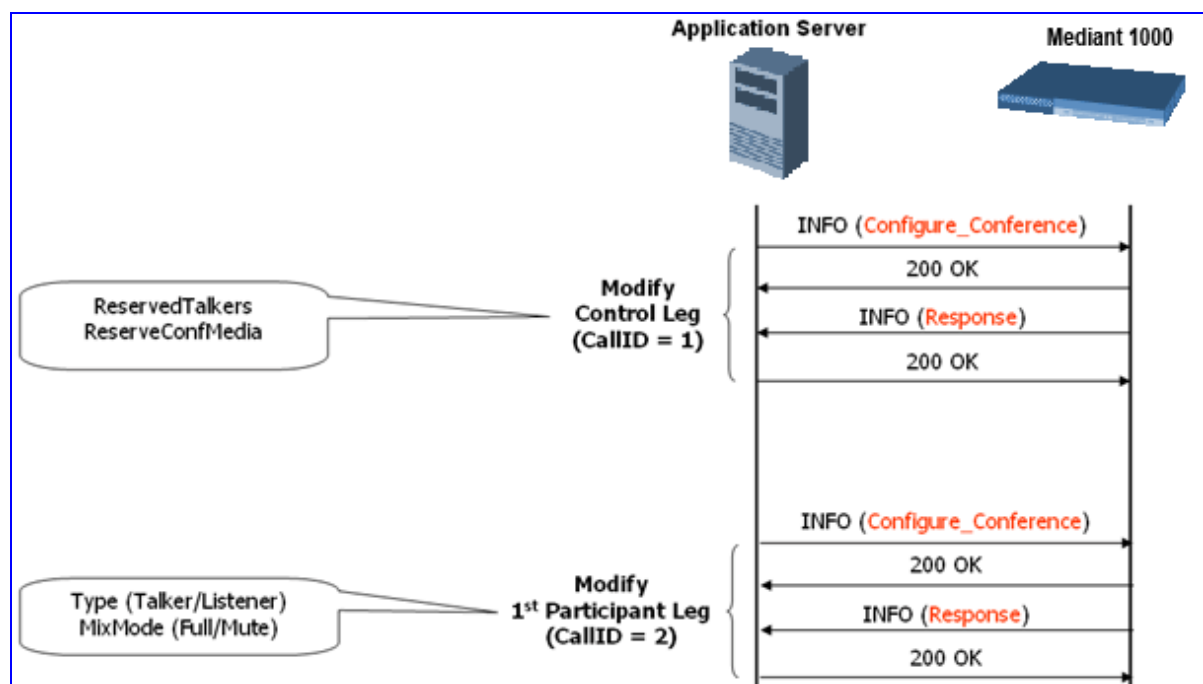
To modify an existing conference, INFO messages are used. Each INFO message carries an MSCML request. The MSCML response is included in an INFO message back from the gateway to the Application Server. It is possible to modify an entire conference (by issuing requests on the Control Leg) or only a certain participant (by issuing requests on that specific leg).

To modify the entire conference, a `<configure_conference>` MSCML request body is sent in an INFO message on the Control Leg SIP dialog. Using this request, the Application Server can modify the following attributes:

- **Reservedtalkers:** If the Application Server sets a number that is lower than the initial number requested in the INVITE, then the request is not granted. If the number is higher than the initial number, the gateway sends a success response in the response INFO.
- **Reserveconfmedia:** If the necessary resources for applying Media Services on the entire conference were reserved in advance, then by setting `reserveconfmedia` to Yes, it is reserved. If set to No, the gateway can free the resource.

To modify a certain Participant Leg, a `<configure_leg>` MSCML request body is sent in an INFO message on that leg SIP dialog. Using this request, the Application Server can modify any of the attributes defined for the `<configure_leg>` request.

Figure 10-3: Modifying a Conference - SIP Call Flow

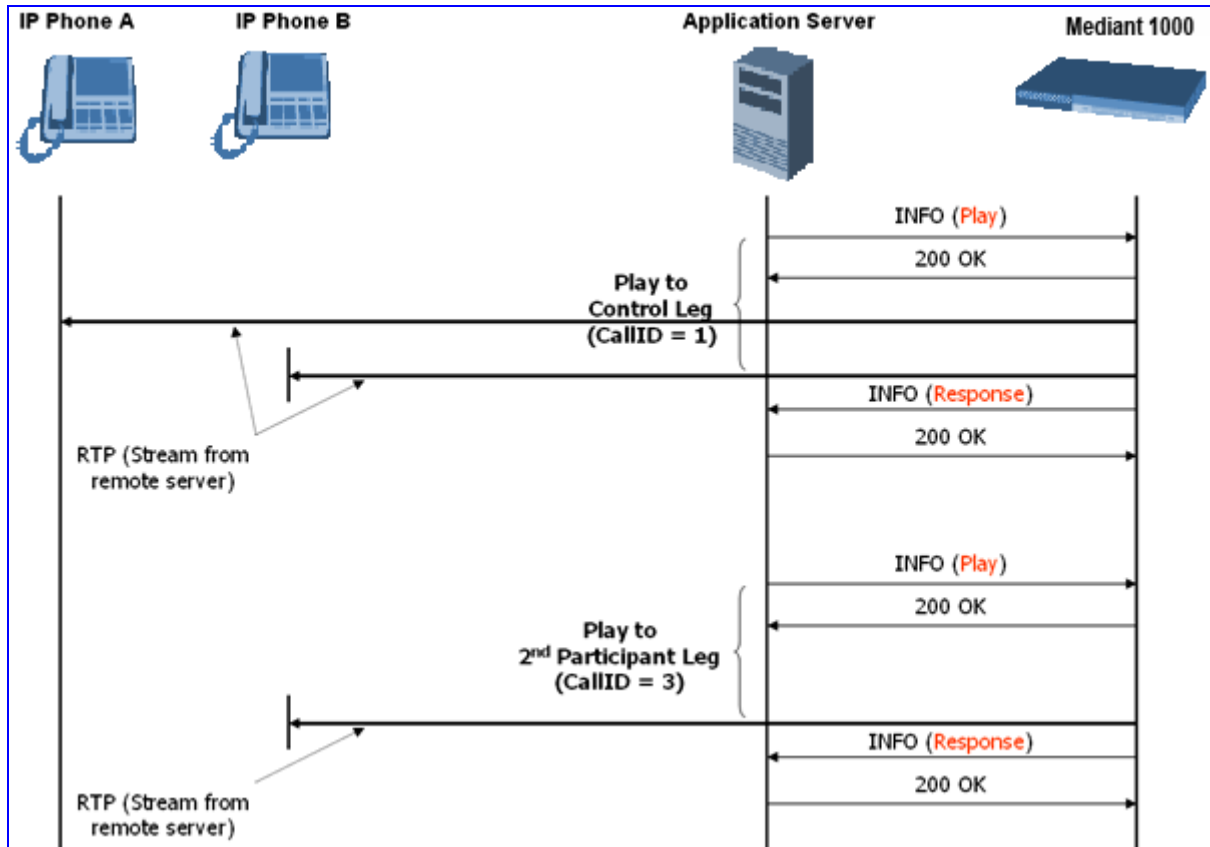


10.1.2.4 Applying Media Services on a Conference

The Application Server can issue a Media Service request (`<play>`, `<playcollect>`, or `<playrecord>`) on either the Control Leg or a specific Participant Leg. For a Participant Leg, all three requests are applicable. For the Control Leg, the `<playcollect>` is not applicable as there is no way to collect digits from the whole conference.

When issuing a Media Service on the Control Leg, it affects all Participant Legs in the conference, e.g., play an announcement. When issuing a Media Service on a Participant Leg, it affects the specific leg only.

Figure 10-4: Applying Media Services on a Conference -- SIP Call Flow



10.1.2.5 Active Speaker Notification

After an advanced conference is established, the Application Server can subscribe to the gateway to receive notifications of the current set of active speakers in a conference at any given moment. This feature is referred to as *Active Speaker Notification (ASN)* and is designed according to the MSCML standard. Notifications provide information on the number of active participants and their details.

The notifications are sent unsolicited at specific intervals requested by the application and only when a change in the number of active conference speakers occurs. If a change in the speakers list occurs, the server issues an INVITE to the specific SIP UA, and then transfers the call to the UA.

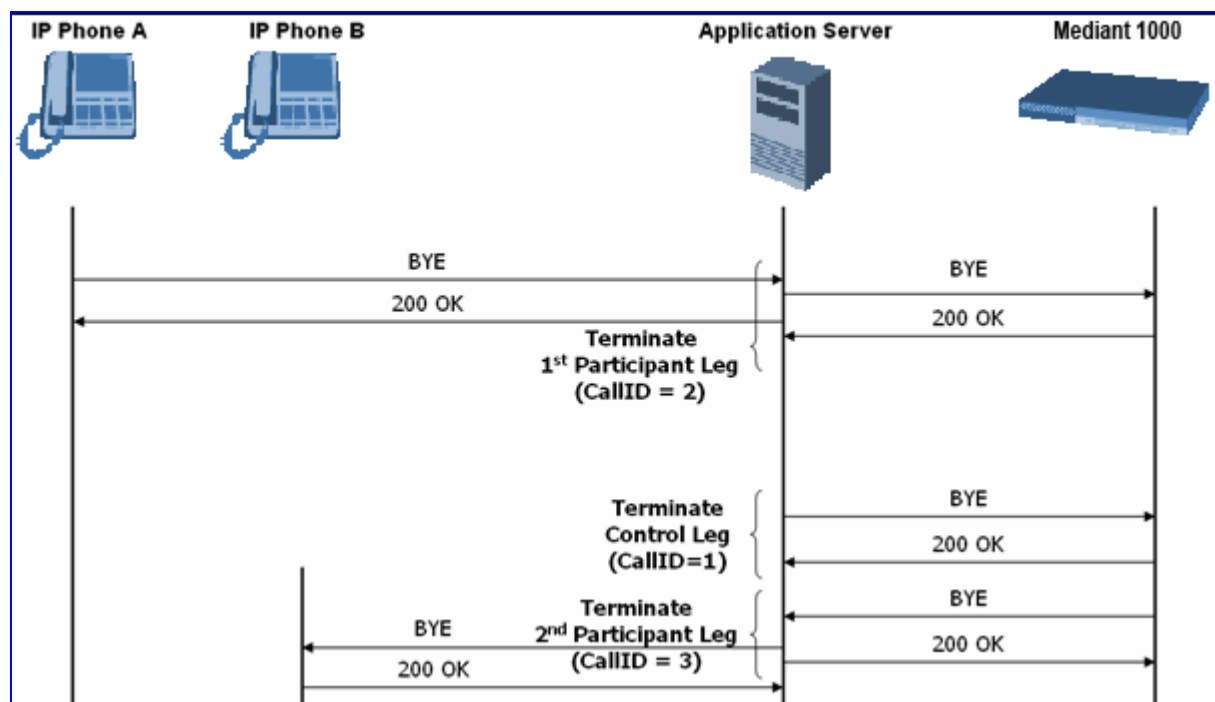
Event notifications are sent in SIP INFO messages, as shown in the example below of XML Response Generated for ASN:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
<notification>
<conference uniqueID="3331" numtalkers="1">
<activetalkers>
<talker callID="9814266171512000193619@10.8.27.118"/>
</activetalkers>
</conference>
</notification>
</MediaServerControl>
```

10.1.2.6 Terminating a Conference

To remove a leg from a conference, the Application Server issues a SIP BYE request on the selected dialog representing the conference leg. The Application Server can terminate all legs in a conference by issuing a SIP BYE request on the Control Leg. If one or more participants are still in the conference when the gateway receives a SIP BYE request on the Control Leg, the gateway issues SIP BYE requests on all of the remaining conference legs to ensure a clean up of the legs.

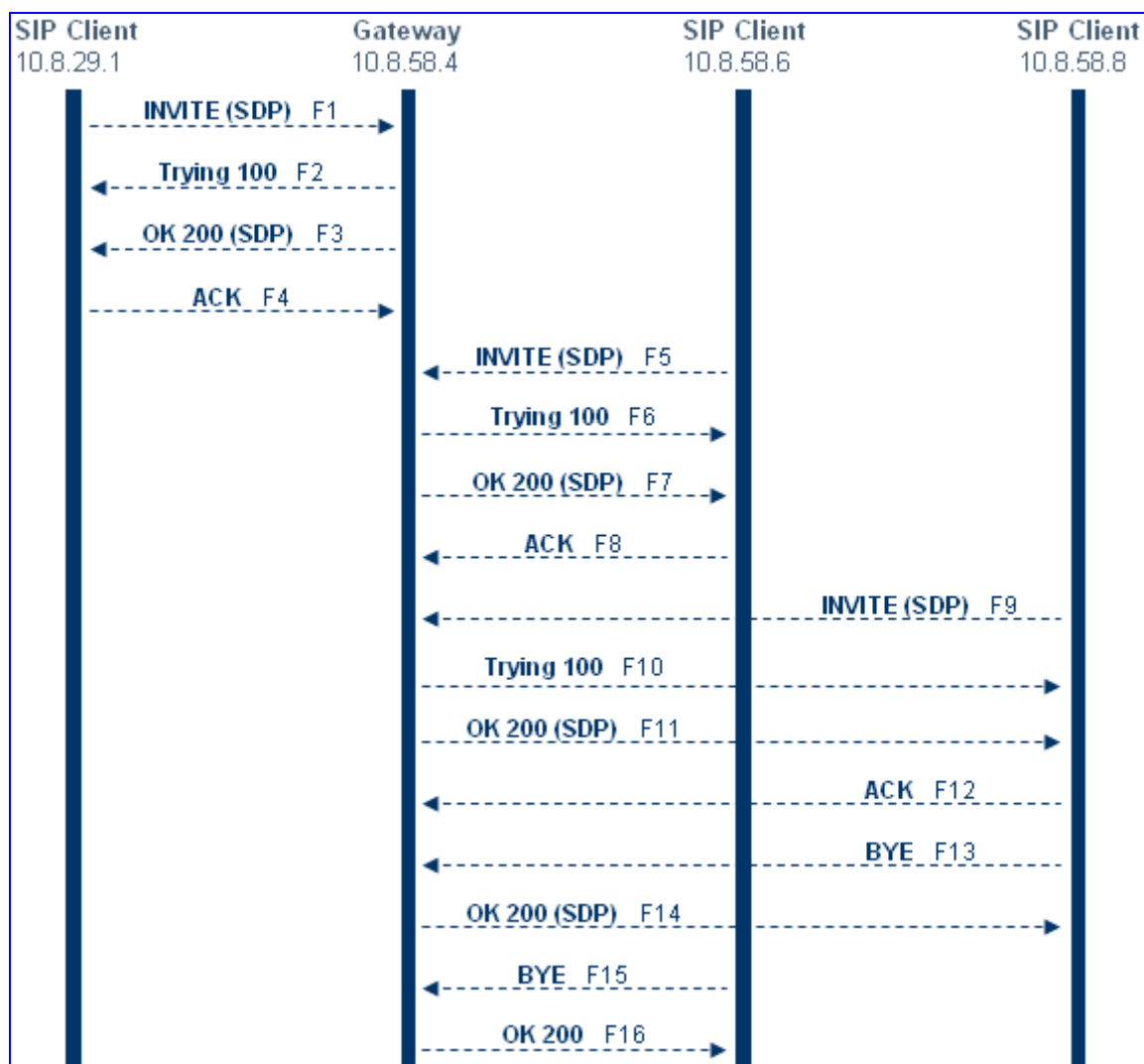
Figure 10-5: Terminating a Conference -- SIP Call Flow



10.1.3 Conference Call Flow Example

The call flow, shown in the following figure, describes SIP messages exchanged between the Mediant 1000 (10.8.58.4) and three conference participants (10.8.29.1, 10.8.58.6 and 10.8.58.8).

Figure 10-6: Conference Call Flow Example



1. SIP MESSAGE 1: 10.8.29.1:5060 -> 10.8.58.4:5060

```
INVITE sip:conf100@10.8.58.4;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.29.1;branch=z9hG4bKacRHmJhMj
Max-Forwards: 70
From: <sip:100@10.8.8.10>;tag=1c352329022
To: <sip:conf100@10.8.58.4;user=phone>
Call-ID: 1792526528qlax@10.8.29.1
CSeq: 1 INVITE
Contact: <sip:100@10.8.29.1>
Supported: em,100rel,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-MP-104 FXS/v.4.60A.006.001
Content-Type: application/sdp
Content-Length: 216
v=0
o=AudiocodesGW 663410 588654 IN IP4 10.8.29.1
s=Phone-Call
c=IN IP4 10.8.29.1
t=0 0
m=audio 6000 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
aptime:20
a=sendrecv
```

2. SIP MESSAGE 2: 10.8.58.4:5060() -> 10.8.29.1:5060()

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.29.1;branch=z9hG4bKacRHmJhMj
From: <sip:100@10.8.8.10>;tag=1c352329022
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c222574568
Call-ID: 1792526528qlax@10.8.29.1
CSeq: 1 INVITE
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-IPMedia 1610/v.4.60A.006.001
Content-Length: 0
```

3. SIP MESSAGE 3: 10.8.58.4:5060 -> 10.8.29.1:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.29.1;branch=z9hG4bKacRHmJhMj
From: <sip:100@10.8.8.10>;tag=1c352329022
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c222574568
Call-ID: 1792526528qlax@10.8.29.1
CSeq: 1 INVITE
Contact: <sip:10.8.58.4>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-IPMedia 1610/v.4.60A.006.001
Content-Type: application/sdp
Content-Length: 216
v=0
o=AudiocodesGW 820775 130089 IN IP4 10.8.58.4
s=Phone-Call
c=IN IP4 10.8.58.4
t=0 0
m=audio 7160 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
aptime:20
a=sendrecv
```

4. SIP MESSAGE 4: 10.8.29.1:5060 -> 10.8.58.4:5060

```

ACK sip:10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.29.1;branch=z9hG4bKacbUrWtRo
Max-Forwards: 70
From: <sip:100@10.8.8.10>;tag=1c352329022
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c222574568
Call-ID: 1792526528qlax@10.8.29.1
CSeq: 1 ACK
Contact: <sip:100@10.8.29.1>
Supported: em,timer,replaces,path
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-MP-104 FXS/v.4.60A.006.001
Content-Length: 0

```

5. SIP MESSAGE 5: 10.8.58.6:5060 -> 10.8.58.4:5060

```

INVITE sip:conf100@10.8.58.4;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacfowEuut
Max-Forwards: 70
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 1 INVITE
Contact: <sip:600@10.8.58.6>
Supported: em,timer,replaces,path
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-MP-112 FXS/v.4.60A.005.009
Content-Type: application/sdp
Content-Length: 313
v=0
o=AudiocodesGW 702680 202680 IN IP4 10.8.58.6
s=Phone-Call
c=IN IP4 10.8.58.6
t=0 0
m=audio 6000 RTP/AVP 4 8 0 110 96
a=rtpmap:4 g723/8000
a=fmtp:4 annexa=no
a=rtpmap:8 pcma/8000
a=rtpmap:0 pcmu/8000
a=rtpmap:110 AMR/8000/1
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:30
a=sendrecv

```

6. SIP MESSAGE 6: 10.8.58.4:5060 -> 10.8.58.6:5060

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacfowEuut
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 1 INVITE
Supported: em,timer,replaces,path
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-IPMedia 1610/v.4.60A.006.001
Content-Length: 0

```

7. SIP MESSAGE 7: 10.8.58.4:5060 -> 10.8.58.6:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacfowEuut
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 1 INVITE Contact: <sip:conf100@10.8.58.4>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-IPMedia 1610/v.4.60A.006.001
Content-Type: application/sdp
Content-Length: 236
v=0 o=AudiocodesGW 886442 597756 IN IP4 10.8.58.4
s=Phone-Call
c=IN IP4 10.8.58.4
t=0 0
m=audio 7150 RTP/AVP 4 96
a=rtpmap:4 g723/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:30
a=sendrecv
```

8. SIP MESSAGE 8: 10.8.58.6:5060 -> 10.8.58.4:5060

```
ACK sip:conf100@10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacRRRZPXN
Max-Forwards: 70
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 1 ACK
Contact: <sip:600@10.8.58.6>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-MP-112 FXS/v.4.60A.005.009
Content-Length: 0
```

9. SIP MESSAGE 9: 10.8.58.8:5060 -> 10.8.58.4:5060

```
INVITE sip:conf100@10.8.58.4;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKaczJpxnnv
Max-Forwards: 70
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 1 INVITE
Contact: <sip:800@10.8.58.8>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-MP-112 FXS/v.4.60A.005.009
Content-Type: application/sdp Content-Length: 236
v=0
o=AudiocodesGW 558246 666026 IN IP4 10.8.58.8
s=Phone-Call
c=IN IP4 10.8.58.8
t=0 0 m=audio 6000 RTP/AVP 4 96
a=rtpmap:4 g723/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:30
a=sendrecv
```

10. SIP MESSAGE 10: 10.8.58.4:5060 -> 10.8.58.8:5060

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKaczJpxnnv
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 1 INVITE
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-IPMedia 1610/v.4.60A.006.001
Content-Length: 0
```

11. SIP MESSAGE 11: 10.8.58.4:5060 -> 10.8.58.8:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKaczJpxnnv
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 1 INVITE
Contact: <sip:conf100@10.8.58.4>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-IPMedia 1610/v.4.60A.006.001
Content-Type: application/sdp
Content-Length: 236
v=0
o=AudiocodesGW 385533 708665 IN IP4 10.8.58.4
s=Phone-Call
c=IN IP4 10.8.58.4
t=0 0
m=audio 7140 RTP/AVP 4 96
a=rtpmap:4 g723/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:30
a=sendrecv
```

12. SIP MESSAGE 12: 10.8.58.8:5060 -> 10.8.58.4:5060

```
ACK sip:conf100@10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKacisqqyow
Max-Forwards: 70
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 1 ACK
Contact: <sip:800@10.8.58.8>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-MP-112 FXS/v.4.60A.005.009
Content-Length: 0
```

13. SIP MESSAGE 13: 10.8.58.8:5060 -> 10.8.58.4:5060

```
BYE sip:conf100@10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKackSIyGww
Max-Forwards: 70
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 2 BYE
Contact: <sip:800@10.8.58.8>
Supported: em,timer,replaces,path
Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, UPDATE
User-Agent: Audiocodes-Sip-Gateway-MP-112 FXS/v.4.60A.005.009
Content-Length: 0
```

14. SIP MESSAGE 14: 10.8.58.4:5060 -> 10.8.58.8:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKackSIyGww
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 2 BYE
Contact: <sip:conf100@10.8.58.4>
Supported: em,timer,replaces,path
Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, UPDATE
Server: Audiocodes-Sip-Gateway-IPMedia 1610/v.4.60A.006.001
Content-Length: 0
```

15. SIP MESSAGE 15: 10.8.58.6:5060 -> 10.8.58.4:5060

```
BYE sip:conf100@10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacQypxnv1
Max-Forwards: 70
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 2 BYE
Contact: <sip:600@10.8.58.6>
Supported: em,timer,replaces,path
Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, UPDATE
User-Agent: Audiocodes-Sip-Gateway-MP-112 FXS/v.4.60A.005.009
Content-Length: 0
```

16. SIP MESSAGE 16: 10.8.58.4:5060 -> 10.8.58.6:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacQypxnv1
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 2 BYE
Contact: <sip:conf100@10.8.58.4>
Supported: em,timer,replaces,path
Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, UPDATE
Server: Audiocodes-Sip-Gateway-IPMedia 1610/v.4.60A.006.001
Content-Length: 0
```

10.2 Announcement Server

The gateway supports playing and recording of announcements (local Voice Prompts or HTTP streaming) and playing of Call Progress Tones over the IP network. Three different methods are available for playing and recording announcements:

- NetAnn for playing a single announcement (refer to 'NetAnn Interface' on page 463)
- MSCML for playing single or multiple announcement(s) and collecting digits' (refer to MSCML' Interface on page 464)

10.2.1 NetAnn Interface

The Mediant 1000 supports playing announcements using NetAnn format (according to RFC 4240).

10.2.1.1 Playing a Local Voice Prompt

To play a single local Voice Prompt, the Application Server (or any SIP user agent) sends a regular SIP INVITE message with SIP URI that includes the NetAnn Announcement Identifier name. For example:

```
INVITE sip:annc@audiocodes.com; play=file://12 SIP/2.0
```

The left part of the SIP URI includes the string 'annc'. In the example above, the gateway starts playing announcement number 12 from the internal Voice Prompts file (file:// and http://localhost formats are supported). The NetAnn Announcement Identifier string is configured using the *ini* file (parameter NetAnnAnncID) or Embedded Web Server (refer to Configuring the IPmedia Parameters). Sending a BYE request terminates the SIP session and stops the playing of the announcement. If the played Voice Prompt reaches its end, the gateway initiates a BYE message to notify the Application Server that the session has ended.

10.2.1.2 Playing using HTTP/NFS Streaming

To play a single announcement via HTTP or NFS streaming, the Application Server (or any SIP user agent) sends a regular SIP INVITE message with SIP URI that includes the NetAnn Announcement Identifier name. For example:

```
INVITE sip:annc@ac.com;  
play=http://server.net/gem/Hello.wav SIP/2.0
```

The left part of the SIP URI includes the string 'annc' terminated by the IP address of the HTTP server, and the name and path of the file to be played. In the example above, the gateway starts playing the 'Hello.wav' file that resides in the folder 'server.net/gem'. The NetAnn Announcement Identifier string is configured using the *ini* file (parameter NetAnnAnncID) or Embedded Web Server (refer to Configuring the IPmedia Parameters). Sending a BYE request terminates the SIP session and stops the playing of the announcement. If the played announcement reaches its end, the gateway initiates a BYE message to notify the Application Server that the session is ended.


Notes:

- A 200 OK message is sent only after the HTTP connection is successfully established and the requested file is found. If the file isn't found, a 404 Not Found response is sent.
- To use NFS, the requested file system should be first mounted by using the NFS Servers table, see Configuring the NFS Settings.

10.2.1.3 Supported Attributes

When playing announcements, the following attributes are available:

- **Repeat:** defines the number of times the announcement is repeated. The default value is 1. The valid range is 1 to 1000, or -1 (i.e., repeats the message forever).
- **Delay:** defines the delay (in msec) between announcement repetitions. The default value is 0. The valid range is 1 to 3,600,000.
- **Duration:** defines the total duration (in msec) the announcement(s) are played. The default value is 0 (i.e., no limitation). The valid range is 1 to 3,600,000.

For example:

```
INVITE sip:annc@ac.com;
play=http://server.net/gem/Hello.wav; repeat=5;delay=10000
SIP/2.0
```

10.2.2 MSCML Interface

Media Server Control Markup Language (MSCML), according to IETF draft <draft-vandyke-mscml-06.txt> is a protocol used in conjunction with SIP to provide advanced announcements handling. MSCML is implemented by adding an XML body to existing SIP INFO messages. Only a single message body (containing a single request or response) is allowed per message.

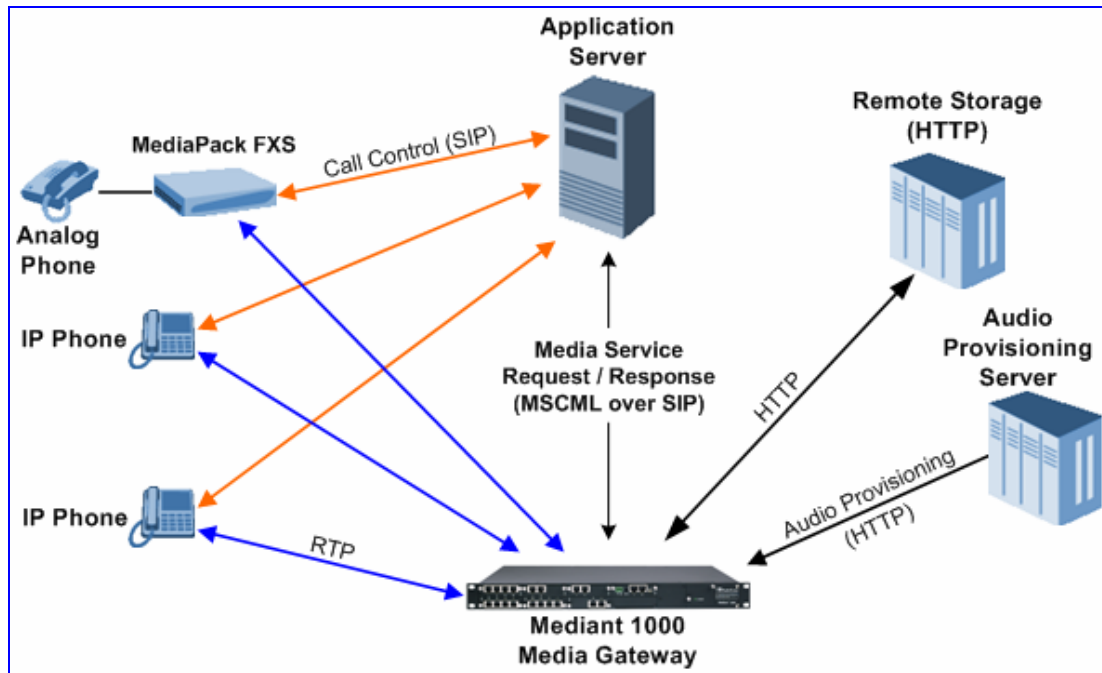
In the current version, the gateway supports all the Interactive Voice Response (IVR) requirements for playing announcements, collecting digits, and recording (Play, PlayCollect, and PlayRecord).



Note: MSCML is only supported on gateways operating with 128-MByte RAM size.

The following figure illustrates standard MSCML application architecture:

Figure 10-7: MSCML Architecture



The architecture comprises the following components:

- **Mediant 1000**: Operating independently, the gateway controls and allocates its processing resources to match each application's requirements. Its primary role is to handle requests from the Application server for playing announcements and collecting digits.
- **Application Server**: An application platform that controls the call signaling. It interfaces with the gateway using MSCML. It instructs the media server to play announcements, collect digits and record voice streams.
- **Audio Provisioning Server (APS)**: The APS provides the gateway with a flexible audio package that enables users to easily import audio files, define audio sequences, and include different languages for variable announcement playing.
- **Remote Storage**: An HTTP server that contains less-frequently used voice prompts for playback and to which voice stream recording is performed.
- **IP Phones / MediaPack**: Client applications.



Note: For detailed information on APS, refer to the following manuals:

- *Audio Provisioning Server User's Manual*, document # LTRT-971xx.
- *Stand Alone APS Installation & Maintenance Manual Version 9.1*, document # RTP-APS09.1.
- *Audio Provisioning Server User's Manual: Audio Files*, document # LTRT-972xx

10.2.2.1 Operation

On startup, the gateway sends a heartbeat packet (a proprietary UDP Ping packet) to the APS. The IP address of the APS to which the gateway sends the heartbeat packet is defined by the parameter HeartBeatDestIP. After receiving the heartbeat packet, the APS scans its internal database for the IP address (node) of the gateway (a provision set that includes all necessary audio data is defined for each node). Once found, the APS sends (over HTTP) the provision set to the gateway. The provision set includes two files: the audio package as a VP.dat file, and an XML file (segments.xml) that contains indices to the announcements stored on the VP.dat file. The two files are stored on the gateway RAM and are used for playing announcements.

An alternative method uses the AutoUpdate mechanism as described in Automatic Update Mechanism. Both the vp.dat and segments.xml file that were previously created using the APS should be located on an external storage server (HTTP, FTP). At startup, the gateway fetches the files from the remote storage. By using the AutoUpdate mechanism, the gateway periodically checks if new files are posted to the remote server and fetches these files.

The Application server communicates with the gateway using MSCML Requests (sent by the Application server), as shown in the example below:

```
<?xml version="1.0" encoding="utf-8"?>
  <MediaServerControl version="1.0">
    <request>
      ... request body ...
    </request>
  </MediaServerControl>
```

The gateway uses MSCML Responses (i.e., sent by the gateway) to reply to the Application server, as shown in the example below:

```
<?xml version="1.0" encoding="utf-8"?>
  <MediaServerControl version="1.0">
    <response>
      ... response body ...
    </response>
  </MediaServerControl>
```

To start an MSCML IVR call, the Application server (or any SIP user agent) sends a regular SIP INVITE message with a SIP URI that includes the MSCML Identifier name. For example:

```
INVITE sip:ivr@audiocodes.com SIP/2.0
```

The left part of the SIP URI includes the MSCML Identifier string 'ivr', which can be configured using the *ini* file (parameter MSCMLID) or Embedded Web Server (refer to Configuring the IPmedia Parameters).

After a call is established, SIP INFO messages are used to carry MSCML requests and responses. An INFO message that carries an MSCML body is identified by its content-type header that is set to 'application/mediaservercontrol+xml'.

Note that IVR requests are not queued. Therefore, if a request is received while another is in progress, the gateway stops the first operation and executes the new request. The gateway generates a response message for the first request and returns any data collected up to that point. If an application is required to stop a request in progress, it issues a <Stop> request. This request also causes the gateway to generate a response message.

The gateway supports basic IVR functions of playing announcements, collecting DTMF digits, and voice stream recording. These services are implemented using the following Request and Response messages:

- <Play> for playing announcements
- <PlayCollect> for playing announcements and collecting digits
- <PlayRecord> for playing announcements and recording voice
- <Stop> for stopping the playing of an announcement

The gateway sends a Response to each Request that is issued by the Application server.

The <Play>, <PlayCollect>, and <PlayRecord> messages are composed of two sections: Attributes and a Prompt block (the request can contain several different Prompt blocks). The Attributes section includes several request-specific parameters. The Prompt block section itself is also composed of two sections: prompt-specific parameters and audio segments (audio / variable). The (optional) prompt-specific parameters include:

- *locale*: defines the language in which the prompt block is played (supported for local files only). For detailed information on language usage, refer to the *Audio Provisioning Server User's Manual* (LTRT-971xx).
- *baseurl*: defines a URL address that functions as a prefix to all audio segment URLs in the Prompt block.

The Prompt block contains references to one or more audio segments. The following audio segment types are available:

- **Physical Audio Segments:** These are physical audio files that are located either locally (on-blade) or on an external HTTP server. If the file is located on-blade, the reference to it is by using one of the following syntaxes:

 'file://x', 'file:///x', 'file:///x' or 'http://localhost/x'

 Where x stands for the file identifier (the ID or alias given by the APS server for local files; or the file's URL in for HTTP streaming).
- **Variables:** These are audio segments whose value is determined at run time. They are defined in the request as a <type, subtype, value> tuple. The gateway transforms the variable data to voice. To support variable playing, APS server support is mandatory. Available variable types are (subtypes in parenthesis): date, duration, month, money (USD), number (crd, ord), digit (gen, ndn) silence, string, time (t12, t24) and weekday.
 It is also possible to store audio files that are required to play supported types of phrases (e.g., dates and times) on an off-board system. This is beneficial in scenarios where the gateway's on-board storage limit has been reached, and thus, additional languages and audio can be stored off-board.
- **Sequences:** These are audio segments that consist of physical audio files and variables. These sequences can be defined using the APS server.

10.2.2.2 Playing Announcements

A <Play> request is used to play an announcement to the caller. Each <Play> request contains a single Prompt block and the following request-specific parameters:

- *id*: an optional random number used to synchronize request and response.
- *prompturl*: a specific audio file URL that is used in addition to the references in the Prompt block. This audio file is the first to be played.

An example of an MSCML <Play> Request that includes local and streaming audio files as well as variables is shown below:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <request>
    <play id="123">
      <prompt>
        <audio url="http://localhost/1"/>
        <variable type="digits" value="284"/>
        <variable type="silence" value="1"/>
        <audio url="http://10.3.0.2/aa.wav"/>
        <audiourl="nfs://10.3.0.3/prov data/bb.wav"/>
      </prompt>
    </play>
  </request>
</MediaServerControl>
```

10.2.2.3 Playing Announcements and Collecting Digits

The <PlayCollect> request is used to play an announcement to the caller and to then collect entered DTMF digits. The play part of the <PlayCollect> request is identical to the <Play> request. The collect part includes an expected digit map. The collected digits are continuously compared to the digit map. Once a match is found, the collected digits are sent in a <PlayCollect> response. The digit map should be in MGCP format (the type value must be set to 'mgcpdigitmap').

For example:

```
<regex type="mgcpdigitmap" value="([0-1]xxx)">
</regex>
```

Each <PlayCollect> request contains the following request-specific parameters in addition to the Prompt block (all parameters are optional):

- *id*: an optional random number used to synchronize request and response.
- *prompturl*: a specific audio file URL that is used in addition to the references in the prompt block. This audio file is the first to be played.
- *barge*: if set to 'NO', DTMF digits received during announcement playback are ignored. If set to 'YES', DTMF digits received during announcement playback stop the playback and start the digit collection phase.
- *firstdigittimer*: defines the amount of time (in milliseconds) the user does not enter any digits, after which a response is sent indicating timeout.
- *interdigittimer*: defines the amount of time (in milliseconds) the user does not enter any digits after the first DTMF digit is received, after which a response is sent indicating timeout.

- *extradigittimer*: used to enable the following:
 - Detection of command keys (ReturnKey and EscapeKey).
 - Not report the shortest match. MGCP Digitmap searches for the shortest possible match. This means that if a digitmap of (123 | 1234) is defined, once the user enters 123, a match is found and a response is sent. If ExtraDigitTimer is defined, the match can also be 1234 because the gateway waits for the next digits. To use ExtraDigitTimer, it must be defined in the request and you must add a "T" to the Digitmap (for example, 'xxT'). The ExtraDigitTimer is only used when a match is found. Before a match is found, the timer used is the InterDigitTimer. Therefore, if the ExtraDigitTimer expires, a "match" response reason is reported -- never a "timeout".
- *maxdigits*: defines the maximum number of collected DTMF digits after which the gateway sends a response.
- *cleardigits*: defines whether or not the gateway clears the digit buffer between subsequent requests.
- *returnkey*: defines a specific digit (including '*' and '#') which (when detected during a collection) stops the collection and initiates a response (that includes all digits collected up to that point) to be sent.
- *escapekey*: defines a specific digit (including '*' and '#') which (when detected during a collection) stops the collection and initiates a response (with no collected digits) to be sent.

An example is shown below of an MSCML <PlayCollect> Request that includes a sequence with variables and an MGCP digit map:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <request>
    <playcollect id="6379" barge="NO" returnkey="#">
      <prompt>
        <audio url="http://localhost/1">
          <variable type="silence" value="1"/>
          <variable type="date" subtype="mdy"
value="20041210"/>
        </audio>
      </prompt>
      <regex type="mgcpdigitmap" value="([0-
1]xxx)">
      </regex>
    </playcollect>
  </request>
</MediaServerControl>
```

An example is shown below of an MSCML <PlayCollect> Response:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <response request="playcollect" id="6478" code="200"
text="OK" digits="4563">
  </response>
</MediaServerControl>
```

10.2.2.4 Playing Announcements and Recording Voice

The <PlayRecord> request is used to play an announcement to the caller and to then record the voice stream associated with that caller. The play part of the <PlayRecord> request is identical to the <Play> request. The record part includes a URL to which the voice stream is recorded. This URL refers to an HTTP server.

Each <PlayRecord> request contains the following request-specific parameters in addition to the Prompt block (all parameters except 'recurl' are optional):

- *id*: an optional random number used to synchronize request and response.
- *prompturl*: a specific audio file URL that is used in addition to the references in the prompt block. This audio file is the first to be played.
- *barge*: if set to 'NO', DTMF digits received during announcement playback are ignored. If set to 'YES', DTMF digits received during announcement playback stop the playback and start the recording phase.
- *cleardigits*: defines whether or not the gateway clears the digit buffer between subsequent requests.
- *escapekey*: defines a specific digit (including '*' and '#') which (when detected during any phase) stops the request and initiates a response.
- *recurl*: the URL on the external storage server to which the RTP stream is sent for recording. This is a mandatory parameter.
- *mode*: defines if the recording 'overwrites' the existing file or 'appends' to it.
- *initsilence*: defines how long to wait for initial speech input before terminating the recording. This parameter may take an integer value in milliseconds.
- *endsilence*: defines how long the gateway waits after speech has ended to stop the recording. This parameter may take an integer value in milliseconds.
- *duration*: the total time in milliseconds for the entire recording. Once this time expires, recording stops and a response is generated.
- *recstopmask*: defines a digit pattern to which the gateway compares digits detected during the recording phase. If a match is found, recording stops and a response is sent.

An example is shown below of an MSCML <PlayRecord> Request:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <request>
    <playrecord id="75899" barge="NO"
    Recurl=nfs://10.11.12.13/save/recordings/11.wav>
      <prompt>
        <audio url="nfs://100.101.102.103/45">
          <variable type="date" subtype="mdy"
            value="20041210"/>
        </audio>
      </prompt>
    </playrecord>
  </request>
</MediaServerControl>
```

An example is shown below of an MSCML <PlayRecord> Response:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <response request="playrecord" id="75899" code="200"
text="OK" reclength="15005">
    </response>
</MediaServerControl>
```

10.2.2.5 Stopping the Playing of an Announcement

The Application server issues a <stop> request when it requires that the gateway stops a request in progress and not initiate another operation. The only (optional) request-specific parameter is id.

The gateway refers to a SIP re-INVITE message with hold media (c=0.0.0.0) as an implicit <Stop> request. The gateway immediately terminates the request in progress and sends a response.

An example is shown below of an MSCML <Stop> Request:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <request>
    <stop id="123">
    </stop>
  </request>
</MediaServerControl>
```

10.2.2.6 Relevant Parameters

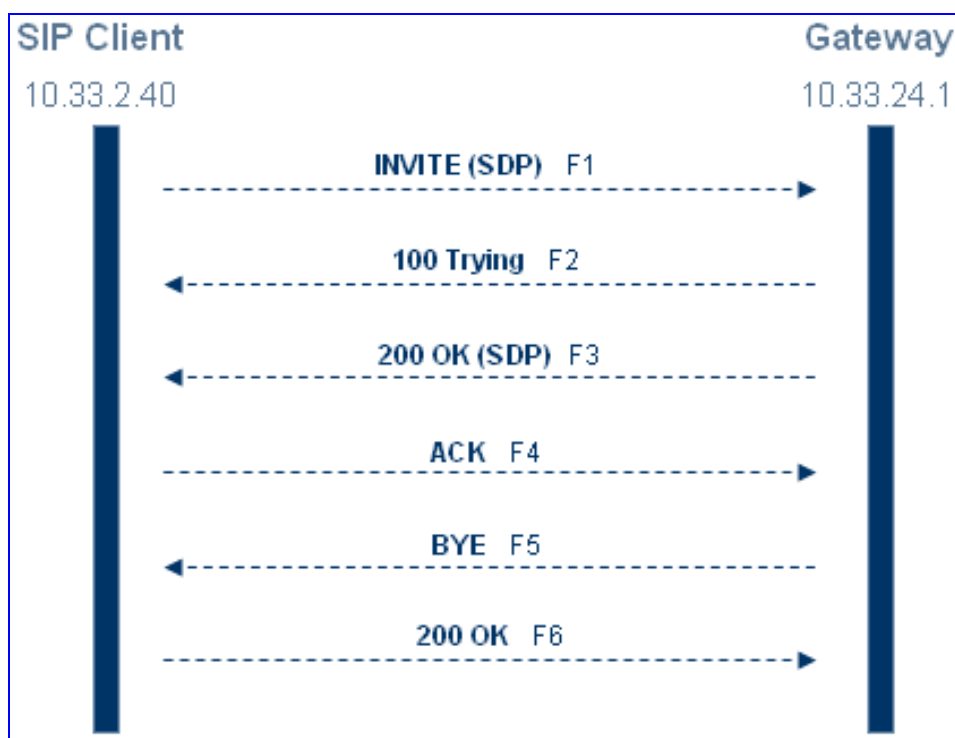
The following parameters (described in Media Server Parameters) are used to configure the MSCML:

- AmsProfile = 1 (mandatory)
- AASPackagesProfile = 3 (mandatory)
- VoiceStreamUploadMethod = 1 (mandatory)
- EnableVoiceStreaming = 1 (mandatory)
- MSCMLID (default="ivr")
- AmsPrimaryLanguage (default="eng")
- AmsSecondaryLanguage (default="heb")
- When using APS:
 - HeartBeatDestIP (refer to System Parameters)
 - HeartBeatDestPort
 - HeartBeatIntervalmsec
- When using AutoUpdate:
 - VPFileURL
 - APSSegmentsFileUrl
 - AutoUpdateFrequency / AutoUpdatePredefinedTime

10.2.3 Announcement Call Flow Example

The call flow, shown in the following figure, describes SIP messages exchanged between an Mediant 1000 (10.33.24.1) and a SIP client (10.33.2.40) requesting to play local announcement #1 (10.8.25.17) using AudioCodes proprietary method.

Figure 10-8: Announcement Call Flow



1. SIP MESSAGE 1: 10.33.2.40:5060 -> 10.33.24.1:5060

```
INVITE
sip:annc@10.33.24.1;play=http://10.3.0.2/hello.wav;repeat=2
SIP/2.0
Via: SIP/2.0/UDP 10.33.2.40;branch=z9hG4bKactXhKPQT
Max-Forwards: 70
From: <sip:103@10.33.2.40>;tag=1c2917829348
To: <sip:annc@10.33.24.1>
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 INVITE
Contact: <sip:103@10.33.2.40>
Supported: em,100rel,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER
,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-4.0 GA/v.4.0 GA
Content-Type: application/sdp
Content-Length: 215
v=0
o=AudiocodesGW 377662 728960 IN IP4 10.33.41.52
s=Phone-Call
c=IN IP4 10.33.41.52
t=0 0
m=audio 4030 RTP/AVP 4 0 8
a=rtpmap:4 g723/8000
a=rtpmap:0 pcmu/8000
a=rtpmap:8 pcma/8000
a=ptime:30
a=sendrecv
```

2. SIP MESSAGE 2: 10.33.24.1:5060 -> 10.33.2.40:5060

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.33.2.40;branch=z9hG4bKactXhKPQT
From: <sip:103@10.33.2.40>;tag=1c2917829348
To: <sip:annc@10.33.24.1>;tag=1c1528117157
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 INVITE
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,
INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-TrunkPack 1610/v.4.60AOH.006.002D
Content-Length: 0
```

3. SIP MESSAGE 3: 10.33.24.1:5060 -> 10.33.2.40:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.33.2.40;branch=z9hG4bKactXhKPQT
From: <sip:103@10.33.2.40>;tag=1c2917829348
To: <sip:annc@10.33.24.1>;tag=1c1528117157
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 INVITE Contact: <sip:10.33.24.1>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER
,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-TrunkPack
1610/v.4.60AOH.006.002D
Content-Type: application/sdp
Content-Length: 165
v=0
o=AudiocodesGW 355320 153319 IN IP4 10.33.24.1
s=Phone-Call
c=IN IP4 10.33.24.1
t=0 0
m=audio 7170 RTP/AVP 0
a=rtpmap:0 pcmu/8000
a=ptime:20
a=sendrecv
```

4. SIP MESSAGE 4: 10.33.2.40:5060 -> 10.33.24.1:5060

```
ACK sip:10.33.24.1 SIP/2.0
Via: SIP/2.0/UDP 10.33.2.40;branch=z9hG4bKacnNUEeKP
Max-Forwards: 70
From: <sip:103@10.33.2.40>;tag=1c2917829348
To: <sip:annc@10.33.24.1>;tag=1c1528117157
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 ACK
Contact: <sip:103@10.33.2.40>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER
,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-4.0 GA/v.4.0 GA
Content-Length: 0
```

5. SIP MESSAGE 5: 10.33.24.1:5060 -> 10.33.2.40:5060

```
BYE sip:103@10.33.2.40 SIP/2.0
Via: SIP/2.0/UDP 10.33.24.1;branch=z9hG4bKacFhtFbFR
Max-Forwards: 70
From: <sip:annc@10.33.24.1>;tag=1c1528117157
To: <sip:103@10.33.2.40>;tag=1c2917829348
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 BYE
Contact: <sip:10.33.24.1>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER
,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-TrunkPack
1610/v.4.60AOH.006.002D
Content-Length: 0
```

6. SIP MESSAGE 6: 10.33.2.40:5060 -> 10.33.24.1:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.33.24.1;branch=z9hG4bKacFhtFbFR
From: <sip:annc@10.33.24.1>;tag=1c1528117157
To: <sip:103@10.33.2.40>;tag=1c2917829348
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 BYE
Contact: <sip:103@10.33.2.40>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER
,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-4.0 GA/v.4.0 GA
Content-Length: 0
```

10.3 IP-to-IP Transcoding

Transcoding is a technology that is used to bridge (translate) between two remote *network* locations each of which uses a different coder and/or a different DTMF and fax transport types. The gateway supports IP-to-IP Transcoding. It creates a Transcoding call that is similar to a dial-in two-party conference call. The SIP URI in the INVITE message is used as a Transcoding service identifier. The Transcoding identifier can be configured using the *ini* file (parameter TranscodingID) or Embedded Web Server (for a description of this parameter, refer to 'Configuring the IPmedia Parameters' on page [175](#)).

It is assumed that the gateway is controlled by a third-party, Application server (or any SIP user agent) that instructs the gateway to start an IP Transcoding call by sending two SIP INVITE messages with SIP URI that includes the Transcoding Identifier name.

For example:

```
Invite sip:trans123@audiocodes.com SIP/2.0
```

The left part of the SIP URI includes the TranscodingID (the default string is 'trans') and is terminated by a unique number (123). The gateway immediately sends a 200 OK message in response to each INVITE.

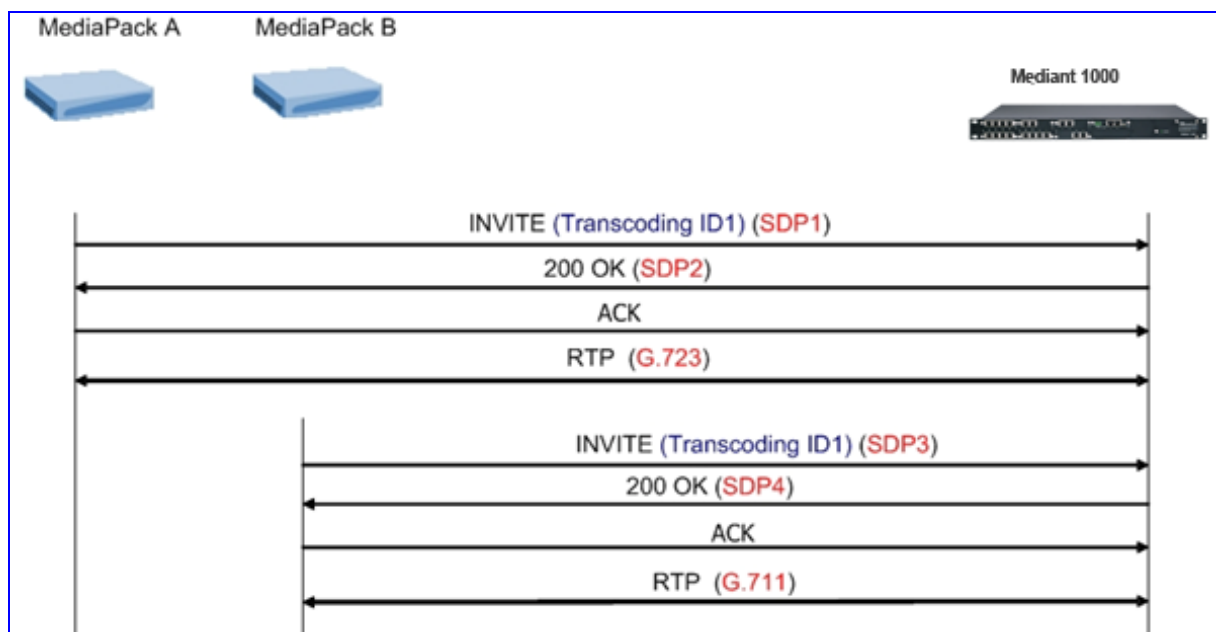
Each of the Transcoding SIP call participants can use a different VoIP coder and a different DTMF transport type, negotiated with the gateway using common SIP negotiation.

Sending a BYE request to the gateway by any of the participants terminates the SIP session and removes it from the Transcoding session. The second BYE from the second participant ends the Transcoding session and releases its resources.

The gateway uses two media (DSP) channels for each call, thereby reducing the number of available Transcoding sessions to half of the defined value for MediaChannels. To limit the number of resources available for the Transcoding, use the *ini* file parameter MediaChannels or Embedded Web Server (refer to 'Configuring the IPmedia Parameters' on page 175). For example, if MediaChannels = 40, only 20 Transcoding sessions are available.

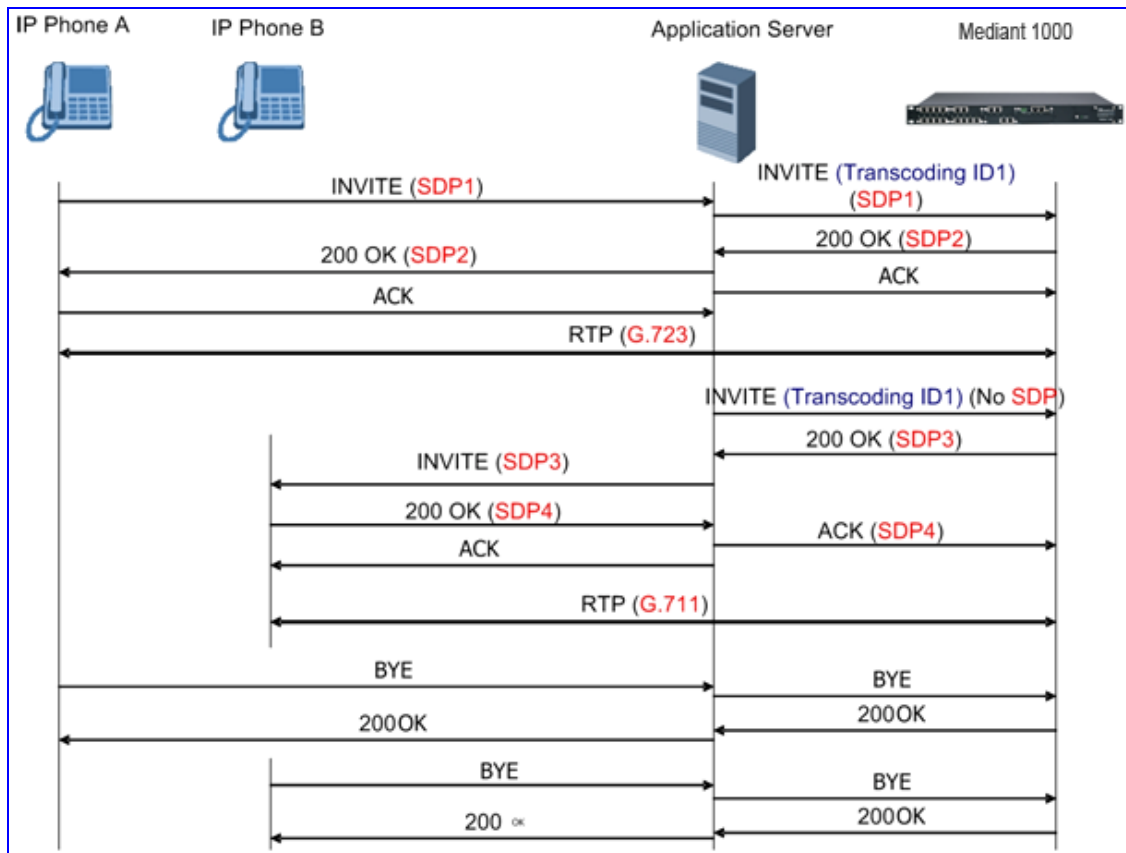
The figure below illustrates an example of a direct connection to a gateway:

Figure 10-9: Direct Connection (Example)



The figure below illustrates an example of implementing an Application server:

Figure 10-10: Using an Application Server (Example)



11 Tunneling Applications

11.1 TDM Tunneling

The gateway TDM Tunneling feature allows you to tunnel groups of digital trunk spans or timeslots (B-channels) over the IP network. TDM Tunneling utilizes the internal routing capabilities of the gateway (without Proxy control) to receive voice and data streams from TDM (1 to 4 E1/T1/J1) spans or individual timeslots, convert them into packets and transmit them automatically over the IP network (using point-to-point or point-to-multipoint gateway distributions). A gateway opposite it (or several gateways when point-to-multipoint distribution is used) converts the IP packets back into TDM traffic. Each timeslot can be targeted to any other timeslot within a trunk in the opposite gateway.

11.1.1 Implementation

When TDM Tunneling is enabled (EnableTDMOverIP is set to 1 on the originating gateway), the originating gateway automatically initiates SIP calls from all enabled B-channels belonging to the E1/T1/J1 spans that are configured with the 'Transparent' protocol (for ISDN trunks), or 'Raw CAS' (for CAS trunks). The called number of each call is the internal phone number of the B-channel that the call originates from. The IP to Trunk Group routing table is used to define the destination IP address of the terminating gateway. The terminating gateway automatically answers these calls if its E1/T1 protocol is set to 'Transparent' (ProtocolType = 5), or 'Raw CAS' (ProtocolType = 3 for T1 and 9 for E1) and the parameter ChannelSelectMode is set to 0 (By Phone Number).



Note: It's possible to configure both gateways to also operate in symmetric mode. To do so, set EnableTDMOverIP to 1 and configure the Tel to IP Routing tables in both gateways. In this mode, each gateway (after it's reset) initiates calls to the second gateway. The first call for each B-channel is answered by the second gateway.

The gateway monitors the established connections continuously, if for some reason one or more calls are released, the gateway automatically reestablishes these 'broken' connections. In addition, when a failure in a physical trunk or in the IP network occurs, the gateways reestablish the tunneling connections as soon as the network restores.



Note: It's recommended to use the keep-alive mechanism for each connection by activating 'session expires' timeout, and using ReINVITE messages.

By utilizing the 'Profiles' mechanism (refer to 'Configuring the Profile Definitions' on page 144) you can configure the TDM Tunneling feature to choose different settings, based on a timeslot or groups of timeslots. For example, you can use low-bit-rate vocoders to transport voice, and 'Transparent' coder to transport data (e.g., for D-channel). You can also use Profiles to assign ToS (for DiffServ) per source, a time-slot carrying data or signaling gets a higher priority value than a time-slot carrying voice.

For tunneling of E1/T1 CAS trunks set the protocol type to Raw CAS (ProtocolType = 3 / 9) and enable RFC 2833 CAS relay mode (CASTransportType = 1).



Note: For TDM over IP, the CallerIDTransportType parameter must be set to 0 (transparent).

Below is an example of *ini* files for two gateways implementing TDM Tunneling for four E1 spans. Note that in this example both gateways are dedicated to TDM tunneling.

Terminating Side:

```
EnableTDMOverIP = 1
;E1_TRANSPARENT_31
ProtocolType 0 = 5
ProtocolType 1 = 5
ProtocolType_2 = 5
ProtocolType_3 = 5
[PREFIX]
FORMAT PREFIX Index = PREFIX DestinationPrefix,
PREFIX DestAddress, PREFIX SourcePrefix, PREFIX ProfileId,
PREFIX MeteringCode, PREFIX DestPort;
Prefix 1 = '*',10.8.24.12';
[\\PREFIX]

; IP address of the gateway in the opposite
; location
; Channel selection by Phone number.
ChannelSelectMode = 0

;Profiles can be used do define different coders per B-channels
;such as Transparent
; coder for B-channels (time slot 16) that carries PRI ;signaling.
[TrunkGroup]
FORMAT TrunkGroup Index = TrunkGroup TrunkGroupNum,
TrunkGroup_FirstTrunkId, TrunkGroup_LastTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId,
TrunkGroup_Module;
TrunkGroup 1 = 0,0,0,1,31,1000,1;
TrunkGroup 1 = 0,1,1,1,31,2000,1;
TrunkGroup 1 = 0,2,2,1,31,3000,1;
TrunkGroup 1 = 0,3,3,1,31,4000,1;
TrunkGroup 1 = 0,0,0,16,16,7000,2;
TrunkGroup 1 = 0,1,1,16,16,7001,2;
TrunkGroup 1 = 0,2,2,16,16,7002,2;
TrunkGroup 1 = 0,3,3,16,16,7003,2;
[/TrunkGroup]
[CoderName]
FORMAT CoderName Index = CoderName Type, CoderName PacketInterval,
CoderName_rate, CoderName_PayloadType, CoderName_Sce;
CoderName 0 = 'g7231';
CoderName 1 = 'Transparent';
CoderName 5 = 'g7231';
CoderName 6 = 'Transparent';
[/CoderName]
[TelProfile]
FORMAT TelProfile Index = TelProfile ProfileName,
TelProfile TelPreference, TelProfile CodersGroupID,
TelProfile_IsFaxUsed, TelProfile_JitterBufMinDelay,
TelProfile_JitterBufOptFactor, TelProfile_IPDiffServ,
TelProfile_SigIPDiffServ, TelProfile DtmfVolume,
TelProfile InputGain, TelProfile VoiceVolume,
TelProfile EnableReversePolarity,
TelProfile EnableCurrentDisconnect,
TelProfile EnableDigitDelivery, TelProfile EnableEC,
```

```

TelProfile MWIAnalog, TelProfile MWIDisplay,
TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia,
TelProfile_ProgressIndicator2IP;
TelProfile 1 = voice,$$,1,$$,,$$,,$$,,$$,,$$;
TelProfile 2 = data,$$,2,$$,,$$,,$$,,$$,,$$,,$$;
[\\TelProfile]

```

Originating Side:

```

;E1 TRANSPARENT 31
ProtocolType_0 = 5
ProtocolType_1 = 5
ProtocolType_2 = 5
ProtocolType_3 = 5
; Channel selection by Phone number.
ChannelSelectMode = 0
[TrunkGroup]
FORMAT TrunkGroup Index = TrunkGroup TrunkGroupNum,
TrunkGroup FirstTrunkId, TrunkGroup LastTrunkId,
TrunkGroup FirstBChannel, TrunkGroup LastBChannel,
TrunkGroup FirstPhoneNumber, TrunkGroup ProfileId,
TrunkGroup Module;
TrunkGroup 0 = 0,0,0,1,31,1000,1;
TrunkGroup 0 = 0,1,1,1,31,2000,1;
TrunkGroup 0 = 0,2,2,1,31,3000,1;
TrunkGroup 0 = 0,3,1,31,4000,1;
TrunkGroup 0 = 0,0,0,16,16,7000,2;
TrunkGroup 0 = 0,1,1,16,16,7001,2;
TrunkGroup 0 = 0,2,2,16,16,7002,2;
TrunkGroup 0 = 0,3,3,16,16,7003,2;
[\\TrunkGroup]
[CoderName]
FORMAT CoderName Index = CoderName Type, CoderName PacketInterval,
CoderName rate, CoderName PayloadType, CoderName Sce;
CoderName 1 = 'g7231';
CoderName 2 = 'Transparent';
[\\CoderName]
[TelProfile]
FORMAT TelProfile_Index = TelProfile_ProfileName,
TelProfile_TelPreference, TelProfile_CodersGroupID,
TelProfile_IsFaxUsed, TelProfile_JitterBufMinDelay,
TelProfile_JitterBufOptFactor, TelProfile_IPDiffServ,
TelProfile_SigIPDiffServ, TelProfile_DtmfVolume,
TelProfile_InputGain, TelProfile_VoiceVolume,
TelProfile_EnableReversePolarity,
TelProfile_EnableCurrentDisconnect,
TelProfile_EnableDigitDelivery, TelProfile_EnableEC,
TelProfile_MWIAnalog, TelProfile_MWIDisplay,
TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia,
TelProfile_ProgressIndicator2IP;
TelProfile_1 = voice,$$,1,$$,,$$,,$$,,$$,,$$
TelProfile_2 = data,$$,2,$$,,$$,,$$,,$$,,$$,,$$
[\\TelProfile]

```

11.2 QSIG Tunneling

The gateway supports QSIG tunneling over SIP according to <draft-elwell-sipping-qsig-tunnel-03>. This method enables all QSIG messages to be sent as raw data in corresponding SIP messages using a dedicated message body. This mechanism is useful for two QSIG subscribers (connected to the same / different QSIG PBX) to communicate with each other over an IP network. Tunneling is supported for both directions (Tel to IP and IP to Tel).

The term tunneling means that messages are transferred 'as is' to the remote side, without being converted (QSIG→SIP→QSIG). The advantage of tunneling over QSIG→SIP interworking is that by using interworking, QSIG functionality can only be partially achieved. When tunneling is used, all QSIG capabilities are supported, whereas the tunneling medium (the SIP network) does not need to process these messages.

11.2.1 Implementation

QSIG messages are transferred in SIP messages in a separate Multipurpose Internet Mail Extensions (MIME) body. Therefore, if a message contains more than one body (e.g., SDP and QSIG), multipart MIME must be used. The Content-Type of the QSIG tunneled message is 'application/QSIG'. In addition, the gateway adds a Content-Disposition header in the following format:

```
Content-Disposition: signal; handling=required.
```

- **Call setup (originating gateway):**

The QSIG SETUP request is encapsulated in a SIP INVITE message without being altered. After the SIP INVITE request is sent, the gateway doesn't encapsulate the following QSIG message until a SIP 200 OK response is received. If the originating gateway receives a 4xx, 5xx or 6xx response, it disconnects the QSIG call with a 'no route to destination' cause.

- **Call setup (terminating gateway):**

After the terminating gateway receives a SIP INVITE request with a Content-Type: application/QSIG, it sends the encapsulated QSIG SETUP message to the Tel side and sends a 200 OK response (no 1xx response is sent) to IP. The 200 OK response includes an encapsulated QSIG CALL PROCEEDING message (without waiting for a CALL PROCEEDING message from the Tel side). If tunneling is disabled and the incoming INVITE includes a QSIG body, a 415 response is sent.

- **Mid-call communication:**

After the SIP connection is established, all QSIG messages are encapsulated in SIP INFO messages.

- **Call tear-down:**

The SIP connection is terminated once the QSIG call is complete. The RELEASE COMPLETE message is encapsulated in the SIP BYE message that terminates the session.

To enable QSIG tunneling set the parameter EnableQSIGTunneling to 1 on both the originating and terminating gateways, and the parameter ISDNDuplicateQ931BuffMode to 128 (duplicate all messages) (both parameters are described in 'ISDN and CAS Interworking-Related Parameters' on page 343).

12 Selected Technical Specifications

The table below lists the main technical specifications of the Mediant 1000.

Table 12-1: Mediant 1000 Functional Specifications

| Function | Specification |
|--------------------------------|---|
| Modularity and Capacity | |
| | <ul style="list-style-type: none"> 6 slots for analog modules, supporting up to 24 FXS/FXO analog ports. Up to 4 digital trunks (fully flexible, up to 4 trunks per module). Note: Channel capacity depends on configuration settings. |
| Interface I/O Modules | |
| FXS Telephony Interface | Up to 6 modules with 4 FXS RJ-11 ports per module (for a total of up to 24 analog FXS RJ-11 ports). |
| FXO Telephony Interface | Up to 6 modules with 4 FXO RJ-11 ports per module (for a total of up to 24 analog FXO RJ-11 ports). |
| Digital Modules | 1, 2, 3 or 4 E1/T1/J1 spans (Balanced 120/100 Ohm) using RJ-48 connectors per module. Up to 4 digital modules (maximum 4 spans per gateway). Optional 1+1 or 2+2 fallback. |
| FXS Functionality | |
| FXS Capabilities | Short or long haul, up to 3,000 m (10,000 ft.), using 24 AWG line cord. |
| | Number of ports per FXS module: 2 or 4 |
| | Caller ID generation: Bellcore GR-30-CORE Type 1 using Bell 202 FSK modulation, ETSI Type 1, NTT, Denmark, India, Brazil, British and DTMF ETSI CID (ETS 300-659-1). |
| | Polarity Reversal and Wink signals generation |
| | Message waiting indication (lamp) |
| | Programmable Line Characteristics: Battery feed, line current, hook thresholds, AC impedance matching, hybrid balance, Tx & Rx frequency response, Tx & Rx Gains Note: For a specific coefficient file, please contact AudioCodes. |
| | Configurable ringing signal: up to three cadences and frequency 10 to 200 Hz. |
| | Drive 4 phones per port simultaneously in offhook and Ring states. REN = 5. |
| | Over-temperature protection for abnormal situations such as shorted lines. |
| | Lifeline on every FXS factory-preconfigured module. |

Table 12-1: Mediant 1000 Functional Specifications

| Function | Specification |
|--|---|
| FXO Functionality | |
| FXO Capabilities | Short or long haul, up to 7,000 m (24,000 ft.), using 24 AWG line cord. |
| | Number of ports per FXO module: 4 |
| | Far-end disconnect detection. |
| | Lightning and high voltage protection for outdoor operation |
| | Programmable Line Characteristics: AC impedance matching, hybrid balance, Tx & Rx frequency response, Tx & Rx Gains, ring detection threshold, DC characteristics Note: For a specific coefficient file, please contact AudioCodes. |
| | Caller ID Detection: Bellcore GR-30-CORE Type 1 using Bell 202 FSK modulation, ETSI Type 1, NTT, Denmark, India, Brazil, British and DTMF ETSI CID (ETS 300-659-1). |
| | Polarity Reversal and Wink signal detection |
| Voice & Tone Characteristics | |
| Voice Compression | G.711 PCM at 64 kbps μ -law/A-law; G.723.1 MP-MLQ at 5.3 or 6.3 kbps; G.726 at 32 kbps ADPCM; G.729 CS-ACELP 8 Kbps Annex A / B; NetCoder at 6.4, 7.2, 8.0 and 8.8 kbps; Microsoft GSM (40 msec) |
| Silence Suppression | G.723.1 Annex A G.729 Annex B PCM and ADPCM - Standard Silence Descriptor (SID) with Proprietary Voice Activity Detection (VAD) and Comfort Noise Generation (CNG). |
| Packet Loss Concealment | G.711 appendix 1; G.723.1; G.729 a/b |
| Echo Canceler | G.165 and G.168 2000, 64 msec |
| Gain Control | Configurable |
| DTMF Transport (in-band) | Mute, transfer in RTP payload or relay in compliance with RFC 2833 |
| DTMF Detection and Generation | Dynamic range 0 to -25 dBm, compliant with TIA 464B and Bellcore TR-NWT-000506. |
| Call Progress Tone Detection and Generation | 32 tones: single tone, dual tones or AM tones, programmable frequency & amplitude; 64 frequencies in the range 300 to 1980 Hz, 1 to 4 cadences per tone, up to 4 sets of ON/OFF periods. |
| Output Gain Control | -32 dB to +31 dB in steps of 1 dB |
| Input Gain Control | -32 dB to +31 dB in steps of 1 dB |
| Conferencing | |
| Module | Optional Media Process module (MPM) housed in Slot 6 on the chassis front panel |
| Conference Channels (Max.) | 60 |

Table 12-1: Mediant 1000 Functional Specifications

| Function | Specification |
|--|---|
| Simultaneous 3-Way Conferences (Max.) | 20 |
| Full-duplex parties per conference bridge ((Max.) | 60 |
| Fax/Modem Relay | |
| Fax Relay | Group 3 fax relay up to 14.4 kbps with auto fallback. T.30 (PSTN) and T.38 (IP) compliant, real time fax relay. Tolerant network delay (up to 9 seconds round trip). CNG tone detection & Relay per T.38. Answer tone (CED or AnsAm) detection & Relay per T.38. |
| Fax Transparency | Automatic fax bypass (pass-through) to G.711, ADPCM or NSE bypass mode |
| Modem Transparency | Auto switch to PCM or ADPCM on V.34 or V.90 modem detection Automatic switching (pass-through) to PCM, ADPCM or NSE bypass mode for modem signals (V.34 or V.90 modem detection). |
| Protocols | |
| VoIP Signaling Protocol | SIP RFC 3261 |
| Communication Protocols | RTP/RTCP packetization. IP stack (UDP, TCP, and RTP). Remote Software load (TFTP, HTTP and HTTPS). |
| Telephony Protocols | PRI (ETSI Euro ISDN, ANSI NI2, 4/5ESS, DMS 100, QSIG, Japan INS1500, Australian Telecom, New Zealand Telecom, Hong Kong Variant, Korean MIC) E1/T1 CAS protocols: MFC R2, E&M wink start, Immediate start, delay start, loop start, ground start, Feature Group B, D for E1/T1 |
| In-Band Signaling | DTMF (TIA 464A) MF-R1, MFC R2 User-defined Call Progress Tones |
| Line Signaling Protocols | Loop start and ground start |
| CPU | |
| Network Interface | Two Ethernet RJ-45 connectors, 10/100 Base-TX |
| RS-232 Interface | RS-232 terminal interface. Non-standard RS-232 connector on the device's CPU. |
| Reset | Resets the device. |
| Dry Contact | NB (Night Bell) and paging |
| Audio I/O | MOH (Music on Hold) and paging |

Table 12-1: Mediant 1000 Functional Specifications

| Function | Specification |
|---|--|
| Physical | |
| Dimensions (W x H x D) | 482.6 mm (19") x 1U x 350.5 mm (13.8") |
| Weight | Approx. 5 kg (depending on number of installed modules) |
| Supply Voltage and Power Consumption | Universal 100 - 240 VAC; 50 - 60 Hz; 1 A max. |
| Environmental | Operational: 0 to 45°C (32 to 113°F) Storage: -10 to 70°C (14 to 158°F) Humidity: 10 to 90% non-condensing |
| Installation | Standard 19-inch rack mount or shelf |
| OSN Server | |
| Single Chassis Integration | Embedded Pentium™ Celeron™ based platform for third-party hosted applications |
| CPU | Intel TM Pentium-M Celeron ULV 600 MHz processor 855 GME + 6300 ESB Intel chipset 128 KB BIOS flash Operational temperature: 0 to 40°C Dimensions (W x H x D): 75 mm (2.9") x 30 mm (1.17") x 160 mm (6.4") Up to 1 Gigabyte 200/266 MHz SODIMM memory. |
| HDD | 40 Gigabyte Hard Disk Drive 5200 RPM (second HDD optional) |
| Interfaces | 10/100 Base-TX, USB, RS-232, NB relay, MOH |
| Diagnostics | |
| Front panel Status LEDs | E1/T1 status LAN status Gateway status (Fail, ACT, Power, and Swap Ready). |
| Syslog events | Supported by Syslog Server (RFC 3164 IETF standard) |
| SNMP MIBs and Traps | SNMP v2c, SNMP v3 |
| Management | |
| Configuration | Gateway configuration using Web browser, CLI or <i>ini</i> files |
| Management and Maintenance | SNMP v2c, SNMP v3 Syslog (according to RFC 3164) Local RS-232 terminal Web Management via HTTP or HTTPS Telnet |

13 Supplied SIP Software Package

The table below lists the supplied standard SIP software package for the Mediant 1000SIP gateways. (The supplied documentation includes this User's Manual and the Release Notes.)

Table 13-1: Supplied Software Package

| File Name | Description |
|---------------------------|--|
| Ram.cmp file | |
| M1000_Digital_SIP_xxx.cmp | Image file containing the software for the Mediant 1000 gateway. |
| M1000_SIP_xxx.cmp | Image file containing the software for both FXS and FXO modules. |
| ini files | |
| SIPgw_M1K.ini | Sample Ini file for the Mediant 1000 media gateway. |
| M1000_Digital_SIP_T1.ini | Sample ini file for Mediant 1000 E1 gateways. |
| M1000_Digital_SIP_E1.ini | Sample ini file for Mediant 1000 T1 gateways. |
| Coeff_FXO.dat | Telephony interface configuration file for FXO modules. |
| Coeff_FXS.dat | Telephony interface configuration file for FXS modules. |
| Usa_tones_xx.dat | Default loadable Call Progress Tones dat file |
| Usa_tones_xx.ini | Call Progress Tones ini file (used to create dat file) |
| Utilities | |
| DConvert | TrunkPack Downloadable Conversion Utility |
| ACSyslog | Syslog server |
| BootP | BootP/TFTP configuration utility |
| CPTWizard | Call Progress Tones Wizard |
| CAS Protocol Files | Used for various signaling types, such as E_M_WinkTable.dat |
| MIB Files | MIB library for SNMP browser |
| CAS Capture Tool | Utility that is used to convert CAS traces to textual form |
| ISDN Capture Tool | Utility that is used to convert ISDN traces to textual form |

Reader's Notes

14 OSN Server Hardware Installation

This section is intended for customers who have purchased the Mediant 1000 media gateway and wish to install the added Mediant 1000 OSN (Open Solution Network) server functionality.

The Mediant 1000 chassis can house a plug-in, OSN Server module for hosting third-party, VoIP applications such as IP-PBX, Pre-Paid, and IP-PBX redundancy. The OSN server is a standalone entity, integrated within the Mediant 1000 gateway, using a separate Ethernet interface and IP configuration as that used by the gateway.

14.1 Required Working Tools

The following tools are required for installing the OSN Server module:

- Phillips screwdriver
- Flathead screwdriver
- Wire cutter

14.2 OSN Server Installation on the Mediant 1000

The Mediant 1000 OSN Server package is composed of three modules, which need to be installed in the Mediant 1000 chassis:

- Connection module (CM)
- iPMX module
- Hard Drive module (HDMX)



Warning: Before installing the Mediant 1000 OSN Server modules, ensure that the Mediant 1000 is disconnected from the power supply. These modules are not hot-swappable and damage to these modules can occur if replaced under voltage.

The OSN Server modules are shown in the figures below:

Figure 14-1: Connection Module (CM)



Figure 14-2: iPMX Module



Figure 14-3: Hard Drive Module (HDMX)



14.2.1 Installing the CM Module

The Connection Module (CM) is installed on the front panel of the Mediant 1000, as described in the following procedure:

➤ **To install the CM module, take these 4 steps:**

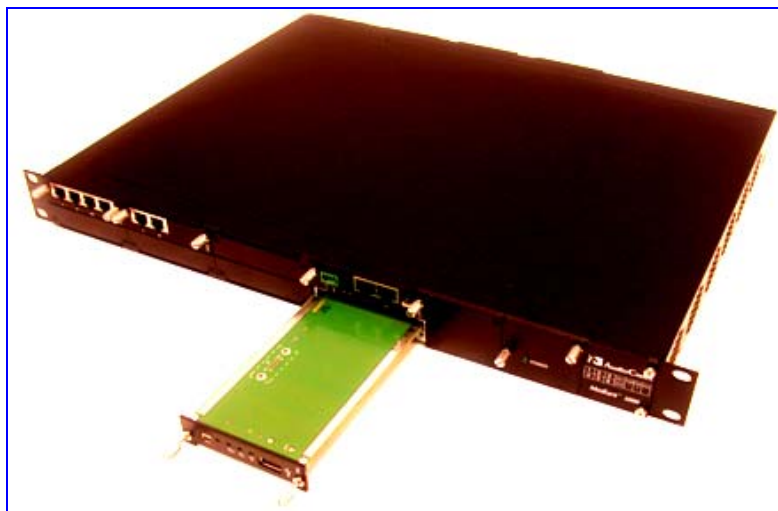
1. On the Mediant 1000 front panel, use a Phillips screwdriver to remove the black metal cover plate from the slot located below the module labeled **CPU**, as shown in the figure below:

Figure 14-4: Mediant 1000 Front Panel



2. Insert the CM module into the empty slot (below the CPU), with the plain side of the Printed Circuit Board (PCB) facing up. Ensure the PCB slides into the slot rails, by aligning the CM with the rails in the slot.

Figure 14-5: Inserting CM Module



3. Gently push the CM module into the slot until it is fully inserted.
4. Using a flathead screwdriver, tighten the module's mounting pins.

14.2.2 Installing the iPMX Module

The iPMX module is installed on the rear panel of the Mediant 1000, as described in the following procedure:

➤ **To install the iPMX module, take these 7 steps:**

1. Place the Mediant 1000 so that the rear panel is facing you, as shown in the figure below.

Figure 14-6: Mediant 1000 Rear Panel



2. Remove the black metal cover plates in the first and second slots located on the right side of the power connection, as shown in the figure below.

Figure 14-7: Mediant 1000 with Cover Plates Removed



3. Use the cutter tool to remove the small metal strip between the upper and lower slots, as shown in the figure below.

Figure 14-8: Mediant 1000 with Cutter Tool



4. Insert the iPMX module into the first slot, closest to the power connection, as shown in the figure below.

Figure 14-9: Inserting iPMX Module



5. Push the iPMX module into the slot and press on it firmly to ensure it has been fully inserted.
6. Using a flathead screwdriver, tighten the module's two captive mounting screws located on the bottom right and left corners.
7. Using a Philips screwdriver, tighten the module's two Philips screws located on the top right and left corners.

14.2.3 Installing the HDMX Module

The Hard Drive module (HDMX) is installed on the rear panel of the Mediant 1000, as described in the following procedure:

➤ **To install the Hard Drive (HDMX) module, take these 6 steps:**

1. Place the Mediant 1000 so that the rear panel is facing you.
2. Remove the black metal cover plates in the first and second slots located on the right side of the power connection.
3. Use the cutter tool to remove the small metal strip between the upper and lower slots.
4. Insert the Hard Drive (HDMX) module into the second slot, as shown in the figure below.

Figure 14-10: Inserting HDMX Module



5. Push the Hard Drive (HDMX) module into the slot and press on it firmly to ensure it has been fully inserted.
6. Using a flathead screwdriver, tighten the module's mounting pins.

14.3 Replacing the iPMX Module's Lithium Battery

The iPMX module is equipped with a 3-volt CR-1225 Lithium battery (AudioCodes product number: ACL P/N RBAT00001). Typically, battery life is estimated at two years. However, for various reasons, the battery may last for a shorter duration.

**Warnings:**

- When replacing the battery, all BIOS settings revert to factory defaults.
- When removing and inserting the battery, be careful not to touch other components on the iPMX printed circuit board (PCB) with the extracting tool. This may cause irreversible damage to the iPMX module.
- Dispose of used batteries according to the manufacturer's instructions. Failure to do so could result in environmental damage.
- The Lithium battery must only be replaced with an identical or equivalent battery, as recommended by the manufacturer.

**Electrical Component Sensitivity**

Electronic components on printed circuit boards are extremely sensitive to static electricity. Normal amounts of static electricity generated by clothing can damage electronic equipment. To reduce the risk of damage due to electrostatic discharge (ESD) when installing or servicing electronic equipment, it is recommended that anti-static earthing straps and mats be used.

The following procedure describes how to replace the Lithium battery in the iPMX module.

➤ **To replace the Lithium battery in the iPMX, take these 6 steps:**

1. Remove the iPMX module from the slot in which it's housed in the Mediant 1000 rear panel, by performing the following:
 - a. Using a flathead screwdriver, loosen the module's two lower mounting captive screws.
 - b. Using a Philips screwdriver, loosen the two upper screws.
 - c. Holding the two mounting captive screws, gently pull the module out of the slot.
2. Flip the module over so that it lies face down with the PCB visible.
3. Locate the Lithium battery in its battery holder on the circuit board.

4. Using a tweezer-like tool (or small flathead screwdriver), carefully leverage the battery out of the battery holder. Be careful not to touch other components on the board with your tool.



5. For installing the new battery, simply push the battery into the battery holder using your fingers. Ensure that you install the battery in the correct orientation such that the positive side is facing up (i.e., the side containing the battery description is visible).
6. Re-insert the iPMX module into the slot of the Mediant 1000 chassis as described in the previous section.

15 Installing Linux™ Operating System on the OSN Server

This appendix describes how to install the following distributions of the Linux™ operating system on the Mediant 1000 OSN server on which the partner application (e.g., IP-PBX) is to run:

- Linux™ RedHat (and Fedora)
- Linux™ Debian
- Linux™ SUSE

This appendix can also serve as a reference for installing other Linux™ distributions. These instructions have been verified against the following distributions:

- RedHat™ Linux 9
- RedHat™ Fedora Core 4
- RedHat™ Enterprise 3
- RedHat™ Enterprise 4
- Debian™ 3.1 (r0a) “Sarge”
- SUSE™ 9.3
- SUSE™ 10



Note: Redhat™ Fedora Core 3 is not supported.

15.1 Requirements

The following subsections list the hardware and software requirements for installing the Linux™ operating system on the Mediant 1000 OSN server.

15.1.1 Hardware

Before installing Linux on the Mediant 1000 OSN Server, ensure you have the following:

- Ethernet cable cord
- External USB CD ROM or DVD ROM (not supplied)
- USB cable (not supplied) to connect the external USB CD ROM to the Mediant 1000
- RS-232 cable (supplied)
- Linux™ Distributions Installation CDs
- Blank CD or DVD media
- Windows™ PC with CD RW or external CD ROM/RW

15.1.2 Software

The software requirements include the following:

- RS-232 console / terminal software (e.g., HyperTerminal™)
- ISO Image Editor (WinISO™ is recommended -- refer to <http://www.winiso.com/download.htm>).
- UNIX™ File Format text editor (refer to <http://www.pspad.com> or <http://www.ultraedit.com>)

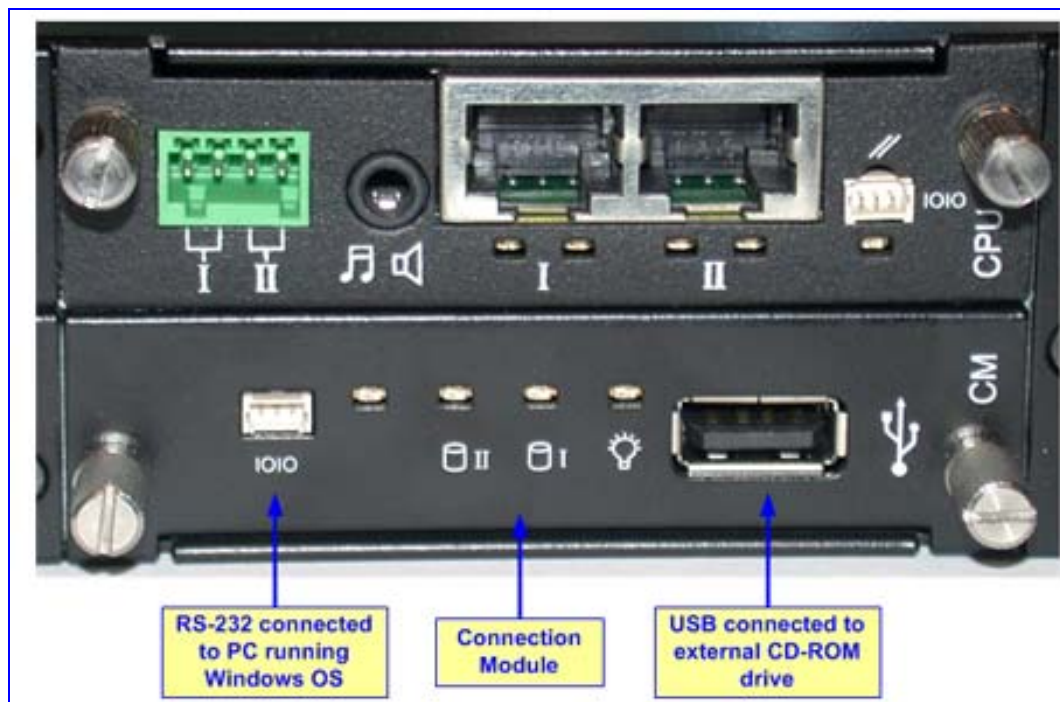
15.2 Cabling

The following procedure describes the cabling before installing Linux™ operating system on the Mediant 1000 OSN Server.

➤ **To cable the OSN Server for installing the Linux™ operating system, take these 4 steps:**

1. On the Mediant 1000 Connection Module (CM) module (located on the front panel), perform the following:
 - a. Connect the RS-232 port to a PC, using the RS-232 cable.
 - b. Connect the USB port to an external CD-ROM drive, using the USB cable.

Figure 15-1: Mediant 1000 Front Panel OSN Server Connections



2. On the Mediant 1000 iPMX module (located on the rear panel), connect the RJ-45 Ethernet port, using the Ethernet cable.
3. Connect the external CD-ROM to the power supply.
4. Connect the Mediant 1000 to the power supply.

15.3 Installing Linux™ RedHat (and Fedora)

Perform the following four stages for installing Linux™ Redhat (and Fedora). (Some distributions of Linux™ may vary slightly):



Notes:

- Some distributions of Linux may vary slightly.
- The Linux version for installation must be according to the application requirements (e.g., Asterisk requires RHAT ES Ver. 3.0; Pingtel ECS requires RHAT ES Ver. 4.0).

15.3.1 Stage 1: Obtaining the Linux Redhat ISO Image

To obtain an updated ISO image, perform one of the following:

- Download it from the AudioCodes Web site, as described in 'Downloading an updated Linux™ Redhat ISO Image' on page 497,
- Create it using the steps detailed in 'Creating an updated Linux Redhat ISO Image' on page 497.

15.3.1.1 Downloading an Updated ISO Image

➤ **To download an ISO image from AudioCodes' Web site, take these 6 steps:**

1. Access AudioCodes' Web site (<http://www.audiocodes.com>), and then navigate to the 'Support' page.
2. Click the **Registered Users Login** link, and then login with your username and password.
3. Under 'Product Documentation', select the **Mediant 1000** link, and then click **Mediant 1000 OSN Server**.
4. Select **Linux Boot Image**, and then select the required installation.
5. Download the ISO image to a folder called 'Partner Install' on your PC.
6. Continue with Stage 3 to burn the CD ('Stage 3: Burn the CD' on page 504).

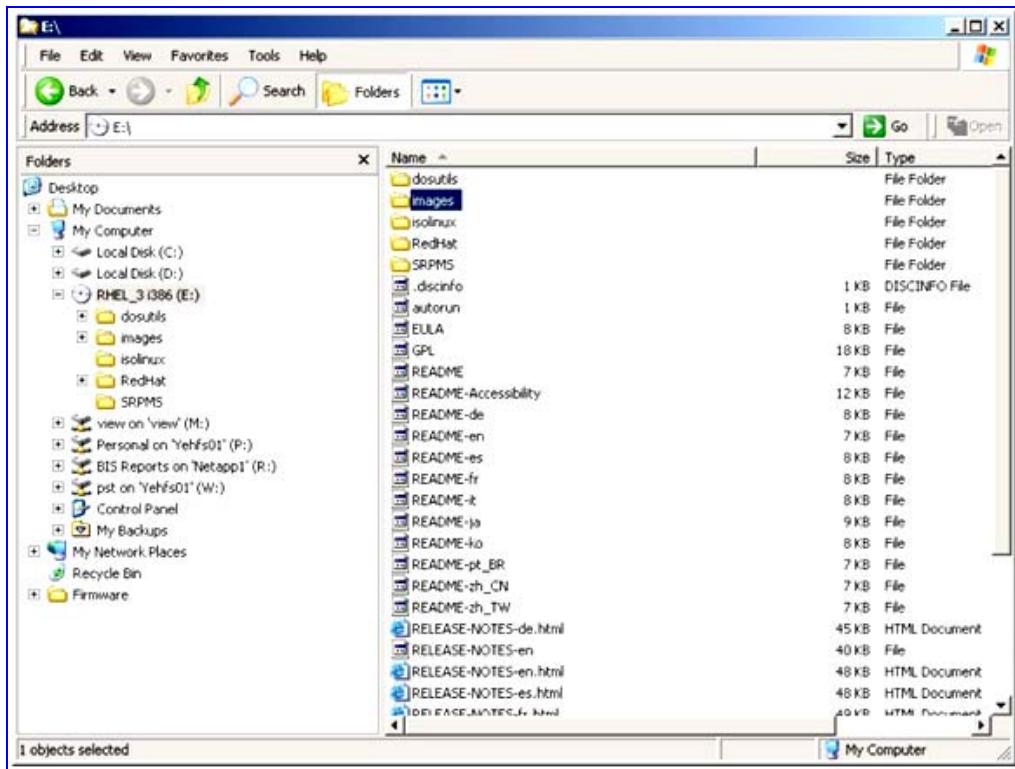
15.3.1.2 Creating an Updated ISO Image

➤ **To create an updated Linux Redhat ISO Image take these 6 steps**

1. On the local hard disk of the Window's™ PC, create a new folder called 'Partner Install'.
2. If you have not already done so, download a utility that allows editing of an ISO image (e.g., WinISO™ from <http://www.winiso.com/download.htm>).

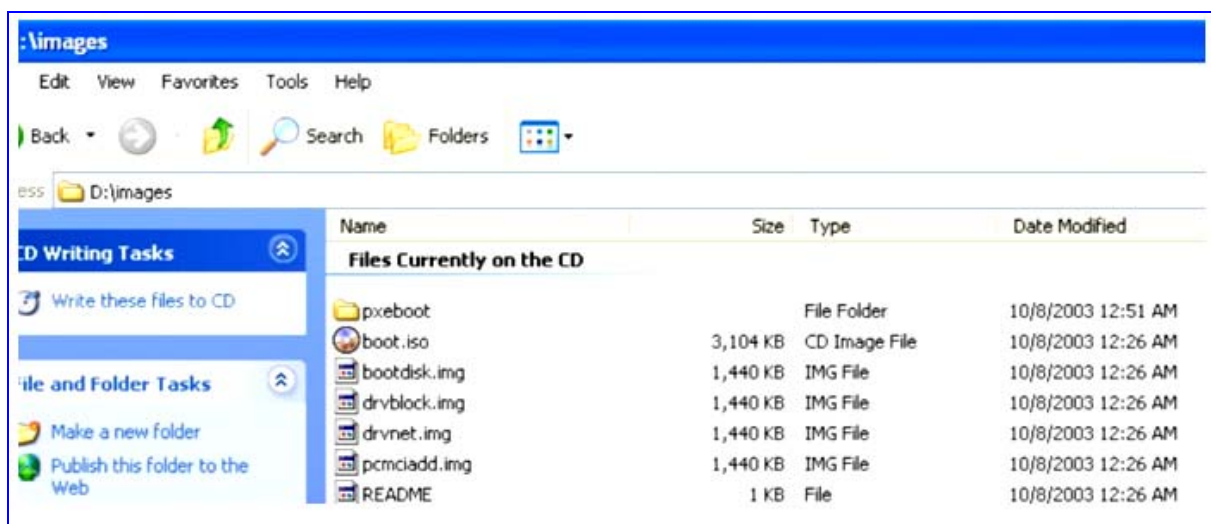
3. Using Internet Explorer, download a UNIX File Format text editor (e.g., PSPad™ at <http://www.pspad.com> or UltraEdit™ at <http://www.ultraedit.com>).
4. Insert the first installation disk of the Linux™ Redhat distribution into the CD-ROM drive of the Windows™ PC. The Windows Explorer screen appears, displaying files currently on the CD.

Figure 15-2: Disk 1 of Redhat Partner Installation



5. Locate the *boot.iso* file in the images folder on the CD (refer to the note below).

Figure 15-3: Images Folder



6. Copy the *boot.iso* file to the 'Partner Install' folder created in Step 1, and then open it with an ISO image editor.

The *isolinux.cfg* file should appear as shown in the screen below.

Figure 15-4: ISO Screen

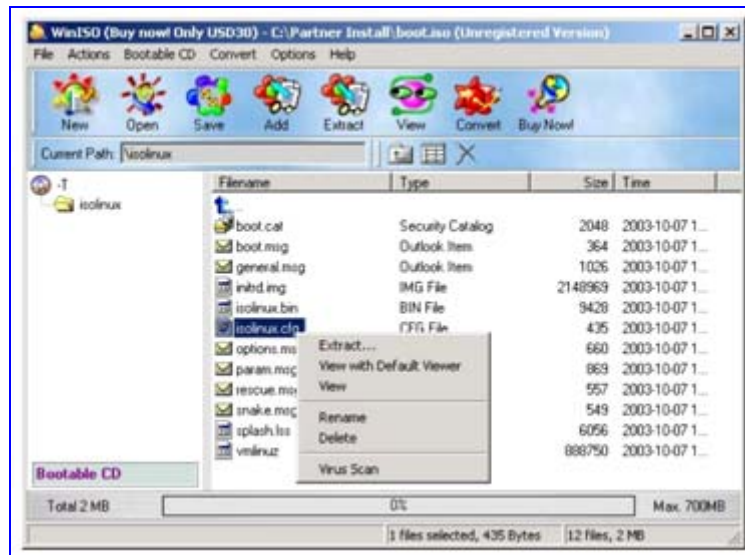


Note: The 'images' folder may be named differently on different Linux™ distributions.

15.3.2 Stage 2: Editing the isolinux.cfg File

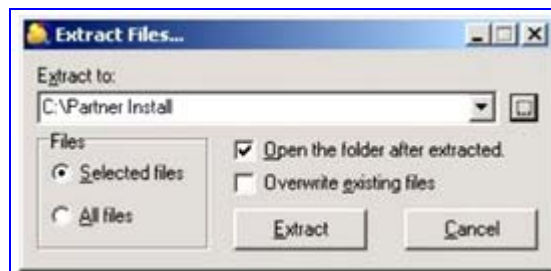
- To edit the *isolinux.cfg* file, take these 14 steps:
- 1. Extract the *isolinux.cfg* file by performing the following:
 - a. Right-click the *isolinux.cfg* file, and then from the shortcut menu, choose **Extract**.

Figure 15-5: Selecting Extract Option



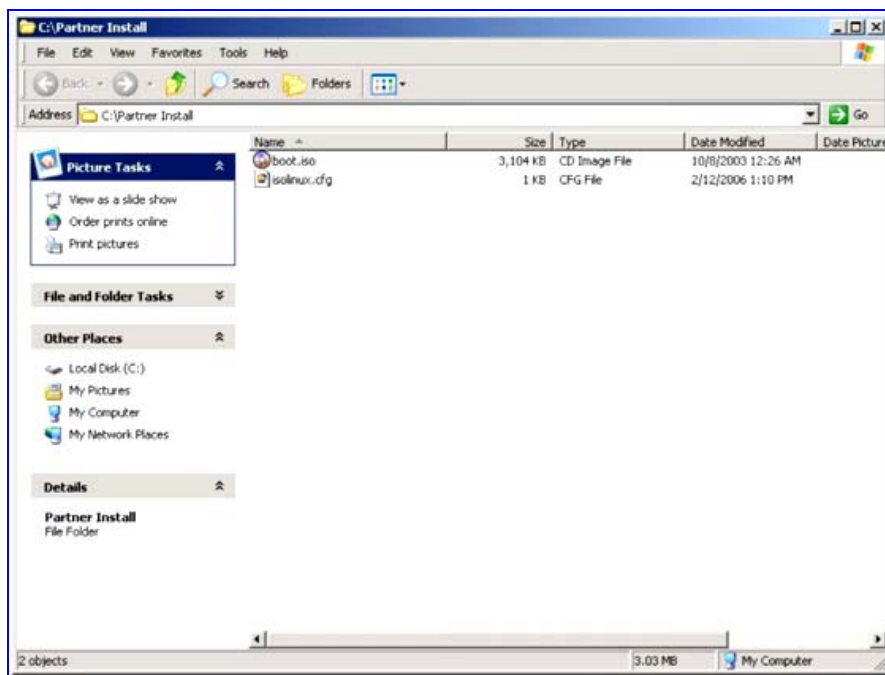
- b. In the 'Extract to' field, browse to the 'Partner Install' folder (created in Stage 1) to where the *isolinux.cfg* file must be extracted.

Figure 15-6: Extracting Files to Partner Install Folder



- c. Click **Extract**; the files is extracted and a screen opens containing the extracted *isolinux* file.

Figure 15-7: ISO-Extract Screen



2. Open the *isolinux.cfg* file with a text editor that supports UNIX file format (e.g., PSPad or UltraEdit); the following screen appears.

Figure 15-8: Text Edit Screen

```
default linux
prompt 1
timeout 600
display boot.msg
F1 boot.msg
F2 options.msg
F3 general.msg
F4 param.msg
F5 rescue.msg
F7 snake.msg
label linux
    kernel vmlinuz
    append initrd=initrd.img
label text
    kernel vmlinuz
    append initrd=initrd.img text
label expert
    kernel vmlinuz
    append expert initrd=initrd.img
label ks
    kernel vmlinuz
    append ks initrd=initrd.img
label lowres
    kernel vmlinuz
    append initrd=initrd.img lowres
```

3. Insert the following line at the beginning of the file so that it's the first line:

```
serial 0 115200
```
4. Locate the line 'default <my_label>' (usually 'default linux' appears), and then locate the line 'label <my_label>' (usually 'label linux' appears). Under this line, the following appears:

```
kernel ...
append ...
```
5. Add the following parameters to the 'append' line of <my_label>:

```
text console=ttyS0,115200
```



Note: In the above string, "ttyS0,115200" consists of a capital "S", only zeros, and one comma.

The 'kerne' and 'append' lines should now look like the following example:

```
label linux
kernel vmlinuz
append initrd=initrd.img ramdisk_size=8192
text console=ttyS0,115200
```

6. Locate the line 'prompt <flag>' (usually 'prompt 1' appears) and change it to 'prompt 0'.
7. Locate the line 'timeout <tenth_of_secs>' (usually 'timeout 600' appears) and change it to 'timeout 0'.



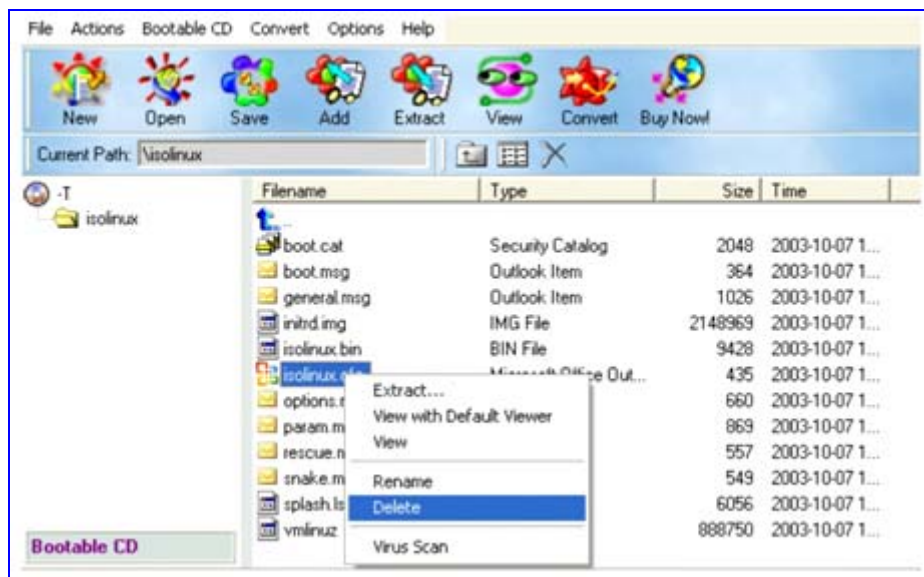
Note: If the timeout line does not exist, **do not** add it.

The *isolinux.cfg* file should now look like the following:

```
serial 0 115200
default linux
prompt 0
...
label linux
kernel vmlinuz
append initrd=initrd.img ramdisk_size=8192
text console=ttyS0,115200
```

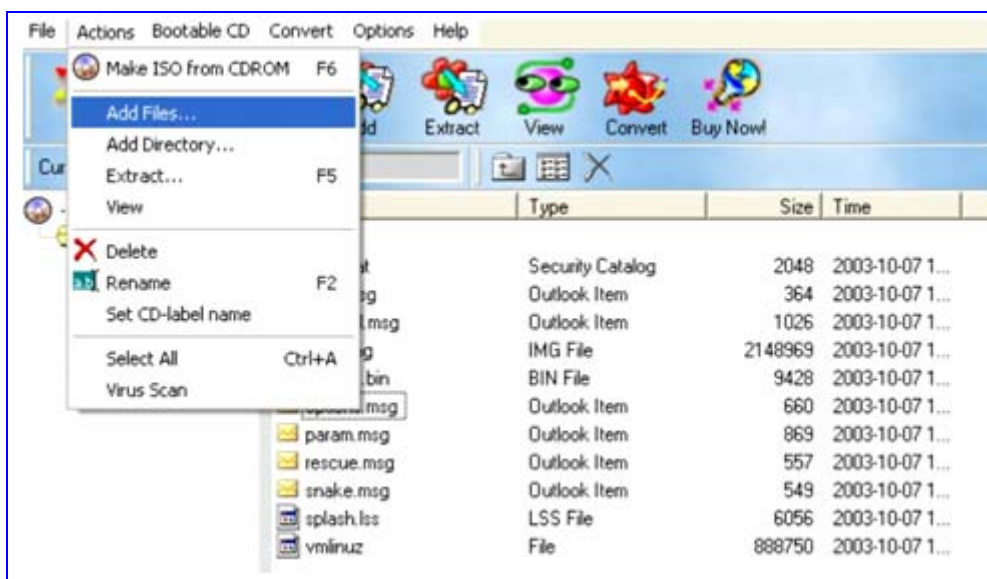
8. Save the changes to the *isolinux.cfg* file, and then close the text editor.
9. Navigate to the 'Partner Install' folder and with the ISO editing utility, open the *boot.iso* file.
10. Double-click the 'isolinux' directory; the folder's contents are displayed.
11. Right-click the *isolinux.cfg* file, and then from the shortcut menu, choose **Delete** to delete this file.

Figure 15-9: Deleting CFG



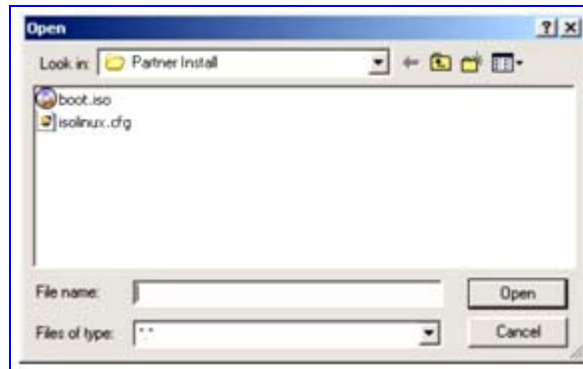
12. From the ISO edit utility menu, select the **Actions** option, followed by **Add Files**.

Figure 15-10: File Add



13. Navigate to the 'Partner Install' folder, select the *isolinux.cfg* file, and then click **Open**.

Figure 15-11: ISO Open Function



The updated *isolinux.cfg* file has now been copied from the 'Partner Install' folder to the *boot.iso* image.

14. Save the *boot.iso* image in the 'Partner Install' folder.

15.3.3 Stage 3: Burning ISO Image File to CD-ROM

➤ **To burn the *boot.iso* file to a CD-ROM, take these 3 steps:**

1. Open a burning utility.
2. Use the **Burn Image** option to burn the *boot.iso* file to an empty CD media.
3. Label the media as "Boot CD".



Note: Ensure that the *boot.iso* file is burned to the CD as an image and not as a data file.

15.3.4 Stage 4: Installing the Boot Media

Now you have the boot media which enables the installation of the Mediant 1000 using the serial connection (terminal) with RS-232 cable.



Note: Some third-party applications require specific Linux OS installation steps. Once you have completed the basic installation procedure explained in this section, refer to the relevant third-party application user's manual for a detailed explanation on installing the Linux OS per third-party application.

➤ **To complete the installation, take these 9 steps:**

1. Connect your Windows™ PC to the Mediant 1000 using a serial cable.
2. Connect the USB CD-ROM device to the Mediant 1000 using a USB cable.
3. Power up the PC.

4. Open the Terminal application (e.g. HyperTerminal) on your Windows™ PC. Create a new connection with the following settings:
 - Connect Port: COM1
 - Baudrate: 115200 (bits per second)
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: None
5. Insert the “Boot CD” (created in Stage 3) into the USB CD-ROM drive.
6. Power up the Mediant 1000.
7. On the Terminal application, the BIOS phase starts and the Linux installation begins. The installation uncompresses the kernel, loads it and its drivers, and then starts the interactive installation.



Note: After the BIOS phase, some badly formatted text may appear on the screen.

8. The first interactive screen should be 'Choose a Language'. Select the language you wish to use.

Figure 15-12: Choose a Language

```

Welcome to Red Hat Enterprise Linux

+-----+ Choose a Language +-----+
|
| What language would you like to use
| during the installation process?
|
| Chinese<Simplified>      #
| Chinese<Traditional>    #
| Czech                   #
| Danish                  #
| Dutch                   #
| English                  #
| French                  #
| German                  #
|
|      +-----+
|      | OK |
|      +-----+
|
+-----+

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen
  
```

9. When prompted for the installation media, **remove the “Boot CD” and insert the first installation disk** and select 'CDROM' as your installation media. From this point on, you should proceed with the screen instructions, as instructed by your Linux™ distributor.

15.3.5 Additional RedHat™ and Fedora™ Installation Notes

Please refer to the following notes for the remaining part of the installation.

1. Select **LILO** as your bootloader where possible, otherwise select GRUB.
2. It is recommended that you disable the firewall when prompted (select “**No Firewall**”).
3. If you forget to disable the firewall during the installation and want to do it after the installation, run the following command:

```
/usr/bin/redhat-config-securitylevel-tui --quiet -disabled
```
4. It is recommended that you assign a **static IP address** to your Mediant 1000. So when the installation has been completed, you will be able to create an SSH remote connection and continue the post-installation configuration.
5. During the bootloader configuration (after you selected which bootloader you want to install), you will be prompted to provide additional text to be appended to the kernel. Ensure that the installation (grub-installer or lilo-installer) recognizes the serial console and contains the following text:

```
console=ttyS0,115200
```
6. If there is no text (i.e. the installer did not recognize the serial console), then insert the following:

```
text console=ttyS0,115200
```
7. Once the installation is complete, you are prompted to re-start the Mediant 1000.



Note: If the installed kernel is version 2.6 or later (Fedora Core 4 or later, RedHat Enterprise 4 or later) then refer to the Post-installation Notes for Kernels 2.6+, below.

15.3.6 Post-installation Notes for Kernels 2.6+ (Fedora™ Core 4+ and RedHat™ EL 4+)

1. When the Mediant 1000 is re-booting and after the BIOS phase, there is a bootloader phase (GRUB or LILO) which starts uncompressing and loading the kernel. After the kernel is loaded the services will start. While the services are loading and the message “**Press ‘I’ to enter interactive startup**” appears, press “I”.
2. Once the hardware has been detected, you will be prompted whether to start each service. For the **syslog service**, select “N” (in order NOT to load it).
3. After you login (either serially or using SSH) to the Mediant 1000, you should disable the syslog service from being started during system startup. To do this, you have to disable the **S**syslog** file located in both /etc/rc3.d and in /etc/rc5.d directories. The file is usually called **S12syslog**.
4. Rename it to K12syslog with the following command.

```
mv S12syslog K12syslog
```

15.4 Installing Linux™ Debian

Perform the following five stages for installing Linux™ Debian.



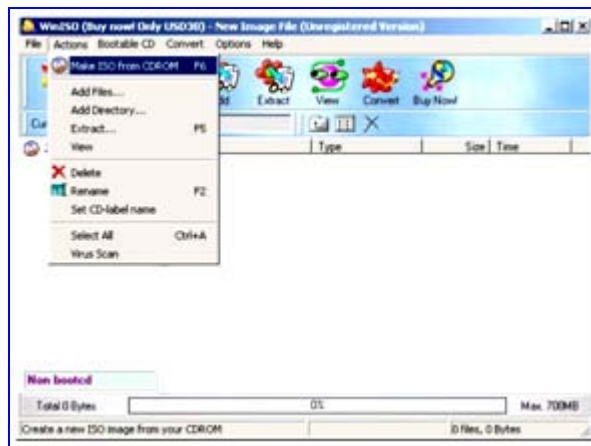
Note: Some distributions of Linux may vary slightly.

15.4.1 Stage 1: Obtaining the ISO Image

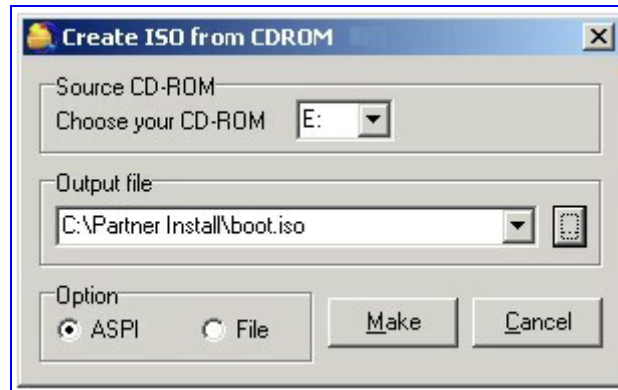
To obtain an updated ISO image, create it using the steps detailed in the section below.

- **To create an ISO image using an ISO editor utility, take these 4 steps:**
 1. Insert the first installation disk of the Linux™ Debian distribution into the CD-ROM drive of the Windows™ PC.
 2. Using Internet Explorer, download a utility that allows editing of an ISO image (e.g., WinISO™ at <http://www.winiso.com/download.htm>).
 3. Start WinISO™, and then from the Actions menu, choose **Make ISO from CDROM**.

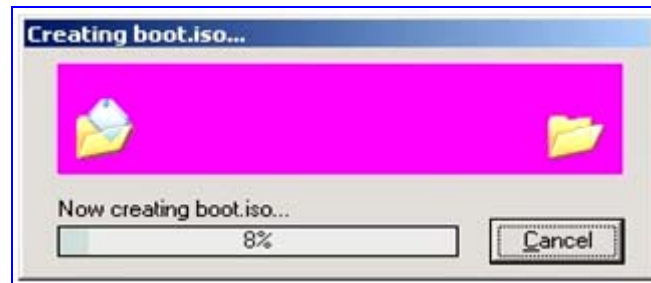
Figure 15-13: WinISO - Actions Screen



4. Create a 'Partner Install' folder on your hard drive. Select **boot.iso** as the output filename, and then click **Make**.

Figure 15-14: Create ISO from CD-ROM


The .iso file starts being created.

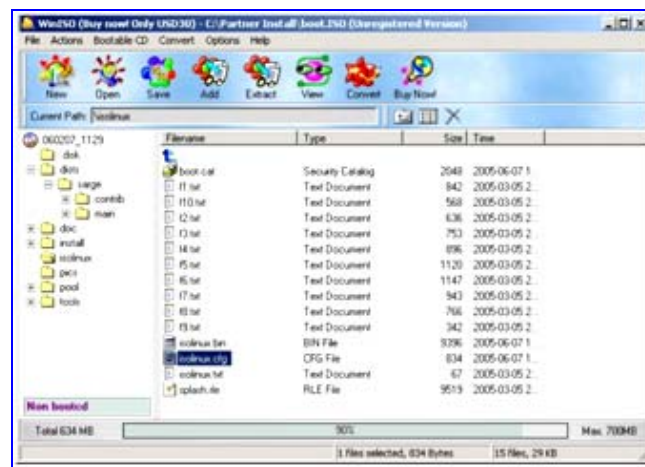
Figure 15-15: Creating .iso File


15.4.2 Stage 2: Preparing the Boot Media

➤ To prepare the Boot Media, take these 5 steps:

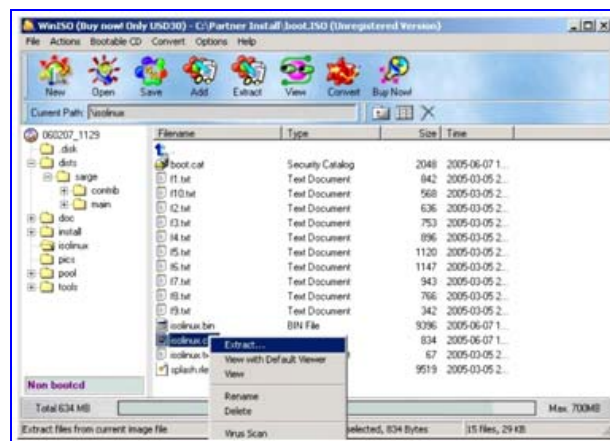
1. If you have not already done so, download a utility that allows editing of an ISO image (e.g., WinISO™ at <http://www.winiso.com/download.htm>).
2. Using Internet Explorer, download a UNIX File Format text editor (e.g., PSPad™ at <http://www.pspad.com> or UltraEdit™ at <http://www.ultraedit.com>).
3. Locate the *boot.iso* file in the 'Partner Install' folder on the hard disk of your PC and with the ISO image utility, navigate to the \isolinux\isolinux.cfg file.

Figure 15-16: Partner Install Folder



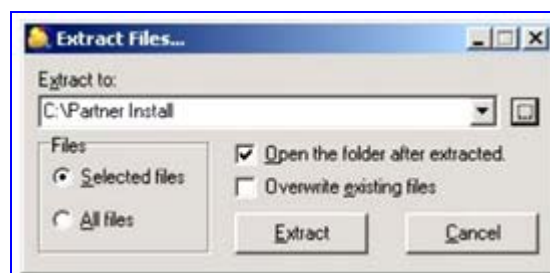
4. Extract the *isolinux.cfg* file by right-clicking the file name, and then from the shortcut menu, choosing **Extract**.

Figure 15-17: Extract isolinux.cfg



5. Extract the *isolinux.cfg* file to the 'Partner Install' folder.

Figure 15-18: Extracting Files to Partner Install Folder



15.4.3 Stage 3: Editing the isolinux.cfg File

To obtain an updated *isolinux.cfg* file, perform one of the following:

- Download it from the AudioCodes Web site as described in 'Downloading an updated Debian isolinux.cfg file' on page 510
- Edit it using the steps detailed in 'Editing the isolinux.cfg File' on page 510

15.4.3.1 Downloading an Updated Debian isolinux.cfg File

➤ **To download an updated Debian isolinux.cfg file from AudioCodes Web site, take these 6 steps:**

1. Access AudioCodes' Web site (<http://www.audiocodes.com>), and then navigate to the 'Support' page.
2. Click the **Registered Users Login** link, and then login with your username and password.
3. Under 'Product Documentation', select the **Mediant 1000** link, and then click **Mediant 1000 OSN Server**.
4. Select **Linux Boot Image**, and then select the required installation.
5. Download the *isolinux.cfg* compressed file to a folder called 'Partner Install' on your PC, and then extract it.
6. Continue with 'Editing the isolinux.cfg File' on page 510.

15.4.3.2 Editing the isolinux.cfg File

➤ **To edit the isolinux.cfg file, take these 12 steps:**

1. Open the 'Partner Install' folder and select the *isolinux.cfg* file with a text editor that supports UNIX file format (e.g., PSPad or UltraEdit).
2. Insert the following line in the beginning of the file, so that it is the first line:
`serial 0 115200`
3. Locate the line 'default <my_kernel>'. It is usually the first line of the file and appears as follows:
`DEFAULT /install/vmlinuz`
Add the following parameters to the 'append' line (located under the 'default' line):
`text console=ttyS0,115200`



Note: In the above string, "ttyS0,115200" consists of a capital "S", only zeros, and one comma.

The 'default <my_kernel>' and 'append' lines should look like the following example:

```
DEFAULT /install/vmlinuz
APPEND vga=normal initrd=/install/initrd.gz text
console=ttyS0,115200 ramdisk_size=10240 root=/dev/rd/0
devfs=mount,dall rw -
```

4. Locate the line 'prompt <flag>' (usually appears as 'prompt 1') and change it to 'prompt 0'.
5. Locate the line 'timeout <tenth_of_secs>' (usually appears as 'timeout 600') and change it to 'timeout 0'.



Note: If the timeout line does not exist, **do not** add it.

The *isolinux.cfg* file should now look like the following:

```
serial 0 115200
DEFAULT /install/vmlinuz

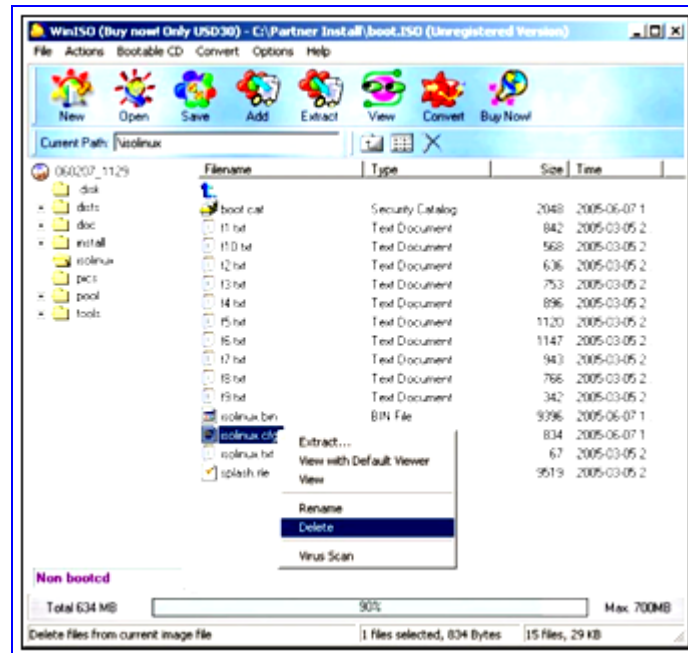
APPEND vga=normal initrd=/install/initrd.gz text
console=ttyS0,115200 ramdisk_size=10240 root=/dev/rd/0
devfs=mount,dall rw --

LABEL linux
kernel /install/vmlinuz
...
DISPLAY isolinux.txt
TIMEOUT 0
PROMPT 0
F1 f1.txt
F2 f2.txt
F3 f3.txt
F4 f4.txt
F5 f5.txt
F6 f6.txt
F7 f7.txt
F8 f8.txt
F9 f9.txt
F0 f10.txt
```

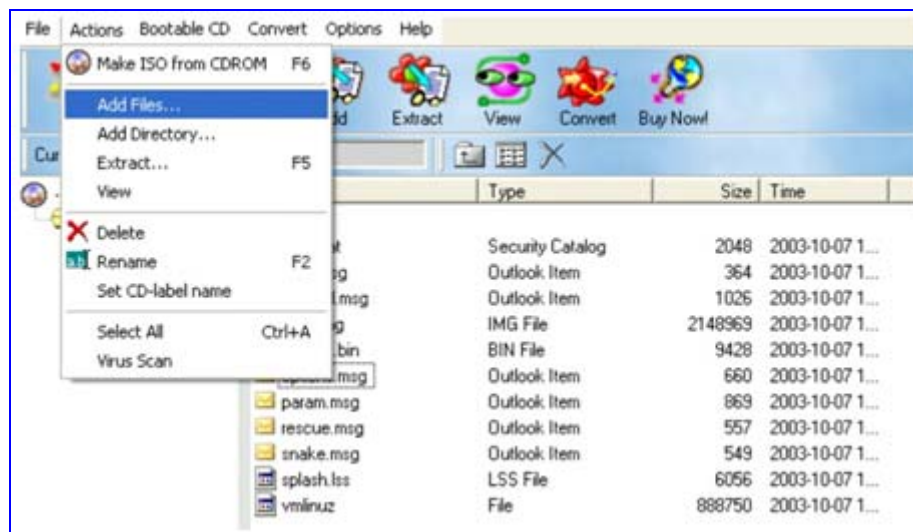


Note: If the timeout line does not exist, do not add it.
 1.If you want to install 'kernel 2.6' rather than the 'default 2.4 version', then:
 a) Take the options from 'kernel' and 'append' lines under the label called 'LABEL linux26'.
 b) Replace the options of 'DEFAULT' and 'APPEND' lines (at the start of the file).
 c) Apply the changes from Step 8..

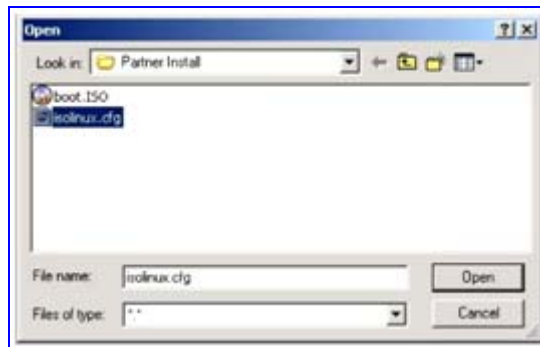
6. Save the changes to the *isolinux.cfg* file, and then close the text editor.
7. Open the 'Partner Install' folder and with the ISO editing utility, open the *boot.iso* file.
8. Click the 'isolinux' directory; the folder's contents appear.
9. Right-click the *isolinux.cfg* file, and then from the shortcut menu, choose **Delete** to delete this file.

Figure 15-19: Deleting CFG


- From the ISO edit utility menu, select the **Actions** option, followed by **Add Files**.

Figure 15-20: File Add


- Navigate to the 'Partner Install' folder, select the *isolinux.cfg* file, and then click **Open**.

Figure 15-21: ISO Open Function

The updated *isolinux.cfg* file is copied to the 'Partner Install\isolinux' directory.

12. Save the *boot.iso* file in the 'Partner Install' folder.

15.4.4 Stage 4: Burning ISO Image to CD

➤ **To burn the boot.iso file to CD, take these 3 steps:**

1. Open a burning utility.
2. Use the **Burn Image** option to burn the *boot.iso* file to an empty CD media.
3. Label the media as the "Boot CD".



Note: Ensure that the *boot.iso* file is burned as an image and not as a data file.

15.4.5 Stage 5: Installing the Boot Media

Now you have the boot media which enables the installation of the Mediant 1000 using the serial connection (terminal) with RS-232 cable.

➤ **To complete the installation, take these 7 steps:**

1. Connect your Windows™ PC to the Mediant 1000 using a serial cable.
2. Connect the USB CD-ROM device to the Mediant 1000 using a USB cable.
3. Power up the PC.

4. Open the Terminal application (e.g. HyperTerminal) on your Windows™ PC. Create a new connection with the following settings:
 - Connect Port: COM1
 - Baudrate: 115200 (bits per second)
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: None
5. Insert the “Boot CD” (created in Stage 3) into the USB CD-ROM drive.
6. Power up the Mediant 1000.
7. On the Terminal application, the BIOS phase starts and the Linux installation begins. The installation uncompresses the kernel, loads it and its drivers, and then starts the interactive installation.


Notes:

- After the BIOS phase, some badly formatted text may appear on the screen.
- From this point on, you should proceed with the screen instructions, as instructed by your Linux distributor.

15.4.6 Additional Linux™ Debian Installation Notes

Please refer to the following notes for the remaining part of the installation.

1. The first interactive screen should be 'Language Selection'. **Before you select the language you wish to use, remove the “Boot CD” and insert the first Debian installation disk.** Select the language you wish to use.
2. As you continue with the installation, you should go through the following stages of the installation:
 - a. Country selection
 - b. CROM scan
 - c. DHCP configuring
3. Configure your network settings manually by selecting the **Configure network manually** option. Either:
 - the DHCP configuration will fail and a screen enabling you to configure the network manually will appear,
 - or -
 - go to the Main Installation menu and select the manual network configuration. Ensure the network is connected and set a **Static IP Address** and all the other network parameters.
4. Continue with the installation, going through the following screens:
 - 'Partition disks'
 - 'Installing the Debian base system'

5. In the 'Install the GRUB boot loader on hard disk' screen, select **Go Back**. This returns you to the 'Debian installer main menu' screen. This is the main menu of the installation.
6. Scroll down in the menu and instead of using GRUB select **Install LILO boot loader on a hard disk**.
7. In the 'LILO Installation target', select **/dev/hda: Master Boot Record**.



Note: The bootloader should detect the serial console. If it doesn't then either:
a) pass additional parameters to the kernel (configure that using the main installation menu)
or/and
b) when configuring LILO you should specify that it tells the kernel to use serial console at speed 115200. In other words append "`text console=ttyS0,115200`" to the kernel options using LILO.
If the serial console wasn't detected during installation, add the following line to the LILO's configuration file after the installation: "`serial=0,115200`"

8. In the next screen, the installation should display the following:
`LILO is configured to use serial port ttyS0 as the console.`
`The serial port speed is set to 115200.`
Select **Continue**; the 'Finish the installation' screen appears followed by 'Installation complete'.
9. Remove the CD and close the CD-ROM drive tray; the system reboots and after the BIOS phase, the kernel starts being uncompressed.
10. The basic installation is now complete. The 'Debian Configuration' screen should appear and this is the phase where you select additional packages to be installed.



Note: Ensure that you install **telnet** and that the **ssh** packages are installed, so that you can connect to your newly-installed system in the future (usually installed by default). From this point on, you should proceed as instructed by your Linux distributor.

11. After the whole installation has been completed, you will be able login to the system from the serial console and/or to "ssh" on your Mediant 1000 (to create an SSH remote connection to it) and to continue its post-installation configuring. You can use the boot media you have created in order to install multiple Mediant 1000 stations.

15.5 Installing Linux™ SUSE

Perform the following five stages for the Linux™ SUSE Installation.



Note: Some distributions of Linux may vary slightly.

15.5.1 Additional Requirement for Linux™ SUSE Installation

To install Linux™ SUSE, a terminal emulation program is required that supports the following:

- ANSI colors (or Linux™ emulation)
- Changing terminal size (to 132x47)

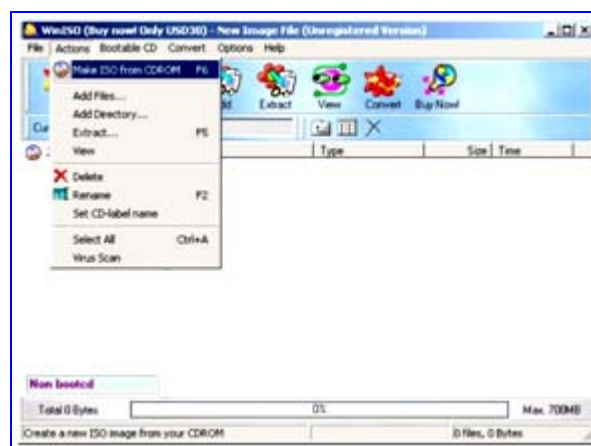
The Tera Term™ program may be used (visit <http://hp.vector.co.jp/authors/VA002416/teraterm.html>).

15.5.2 Stage 1: Obtaining the ISO Image

To obtain an updated ISO image, create it using the procedure described below.

- **To create an ISO image using an ISO editor utility, take these 4 steps:**
 1. Insert the first installation disk of the Linux™ SUSE distribution into the CD-ROM drive of the Windows™ PC.
 2. Using Internet Explorer, download a utility that allows editing of an ISO image (e.g., WinISO™ at <http://www.winiso.com/download.htm>).
 3. Start WinISO™, and then from the **Actions** menu, select **Make ISO from CDRom**.

Figure 15-22: WinISO - Actions Screen



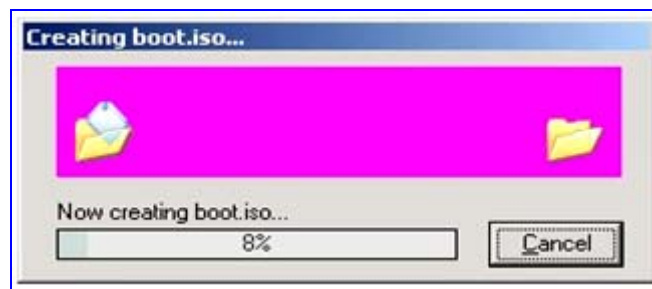
4. Create a 'Partner Install' folder on your hard drive. Select *boot.iso* as the output filename, and then click **Make**.

Figure 15-23: Create ISO from CD-ROM



The utility begins creating the *boot.iso* file.

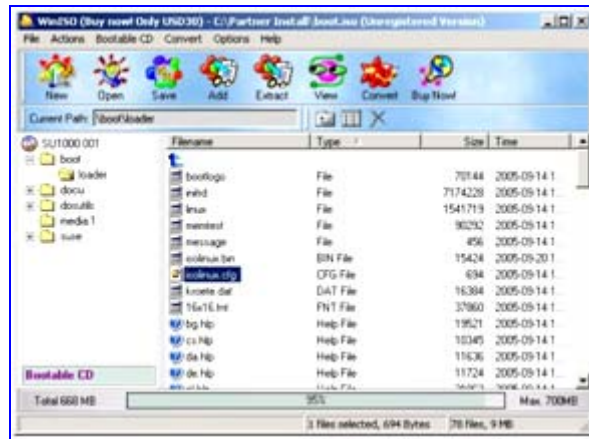
Figure 15-24: Creating .iso File



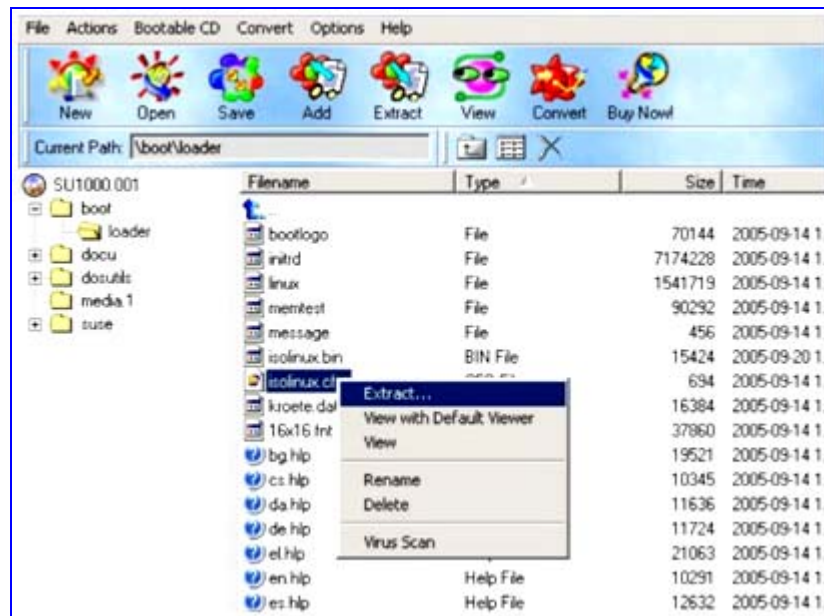
15.5.3 Stage 2: Preparing the Boot Media

➤ **To prepare the Boot Media, take these 5 steps:**

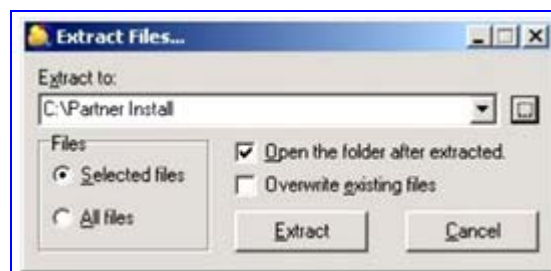
1. If you have not already done so, download a utility that allows editing of an ISO image (e.g., WinIso™ at <http://www.winiso.com/download.htm>).
2. Using Internet Explorer, download a UNIX File Format text editor (e.g., PSPad™ at <http://www.pspad.com> or UltraEdit™ at <http://www.ultraedit.com>).
3. Locate the *boot.iso* file in the 'Partner Install' folder on the hard disk of your PC and navigate to the *isolinux.cfg* file.

Figure 15-25: Partner Install Folder


4. Extract the *isolinux.cfg* file by right-clicking the filename, and then from the shortcut menu, choosing **Extract**.

Figure 15-26: Extract isolinux.cfg File


5. Extract the *isolinux.cfg* file to the 'Partner Install' folder.

Figure 15-27: Extracting Files to Partner Install Folder


15.5.4 Stage 3: Editing the isolinux.cfg File

To obtain an updated isolinux.cfg file, perform one of the following:

- Download it from the AudioCodes Web site as described in 'Downloading an updated SUSE isolinux.cfg file' on page 519
- Edit it using the steps detailed in 'Editing the isolinux.cfg File' on page 520

15.5.4.1 Downloading an Updated SUSE isolinux.cfg File

➤ **To download an updated SUSE isolinux.cfg file from AudioCodes Web site, take these 6 steps:**

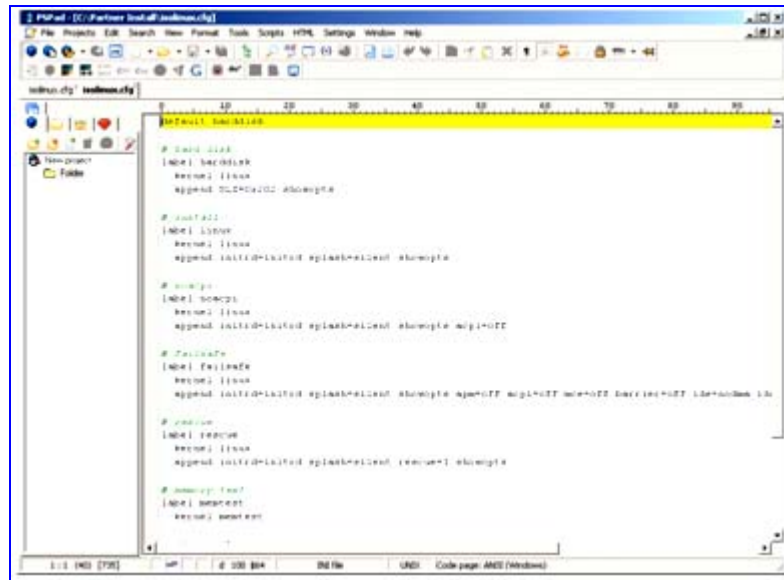
1. Access AudioCodes' Web site (<http://www.audiocodes.com>), and then navigate to the 'Support' page.
2. Click the **Registered Users Login** link, and then login with your username and password.
3. Under 'Product Documentation', select the **Mediant 1000** link, and then click **Mediant 1000 OSN Server**.
4. Select **Linux Boot Image**, and then select the required installation.
5. Download the *isolinux.cfg* compressed file to a folder called 'Partner Install' on your PC and extract it.
6. Continue with 'Editing the isolinux.cfg File' on page 520.

15.5.4.2 Editing the isolinux.cfg File

➤ **To edit the isolinux.cfg file, take these 19 steps:**

1. From the 'Partner Install' folder, open the *isolinux.cfg* file with a text editor that supports UNIX file format (e.g., PSPad or UltraEdit).

Figure 15-28: isolinux.cfg File



2. Insert the following line at the beginning of the file, so that it is the first line.
serial 0 115200
3. Locate the line 'DEFAULT <my_label>' (usually the first line of the file, e.g., 'default harddisk' or 'default linux'.
4. If <my_label> isn't 'linux' (for instance it can be 'harddisk'), change it to 'linux'.
5. Locate the following line: 'label linux'.
6. Under the 'label linux' line, two lines should appear.
kernel...
append...
The following examples show how the 'label linux' line and its 'kernel' and 'append' sublines may appear before you change them:
label linux
kernel linux
append initrd=initrd splash=silent showopts
or
label linux
kernel linux
append initrd=initrd ramdisk_size=65536 splash=silent showopts
7. Remove the 'splash=...' and 'showopts' parameters, if they appear in the 'append' line.



Note: Do not remove any other parameters in the 'append' line, especially the 'initrd=' parameter.

8. Add the following parameters to the 'append' line:

```
text console=ttyS0,115200.
```



Note: In the above string, “ttyS0,115200” consists of a capital “S”, only zeros, and one comma.

The following examples show how the 'label linux' line and its 'kernel' and 'append' sublines may appear after you change them:

```
label linux
  kernel linux
  append initrd=initrd text console=ttyS0,115200
or
label linux
  kernel linux
  append initrd=initrd ramdisk_size=65536 text
  console=ttyS0,115200
```

9. Locate the line 'prompt <flag>' (usually appears as 'prompt 1') and then change it to 'prompt 0'.
10. Locate the line 'timeout <tenth_of_secs>' (usually appears as 'timeout 200') and then change it to 'timeout 0'.



Note: If the timeout line does not exist, **do not** add it.

The *isolinux.cfg* file should now look like the following:

```
serial 0 115200
default linux

# hard disk
label hddisk
  kernel linux
  append SLX=0x202 showopts

# install
label linux
  kernel linux
  append initrd=initrd text console=ttyS0,115200

# noacpi
label noacpi
  kernel linux
  append initrd=initrd splash=silent showopts acpi=off

# failsafe
label failsafe
  kernel linux
  append initrd=initrd splash=silent showopts apm=off acpi=off
  mce=off barrier=off ide=nodma idewait=50 i8042.nomux
  psmouse.proto=bare irqpoll

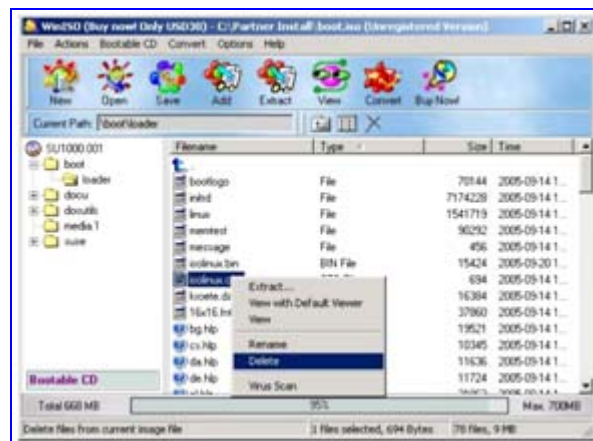
# rescue
label rescue
  kernel linux
  append initrd=initrd splash=silent rescue=1 showopts
```

```
# memory test
label memtest
    kernel memtest

implicit      1
gfxboot      bootlogo
display      message
prompt       0
timeout      0
readinfo     2
framebuffer  1
notice       2
```

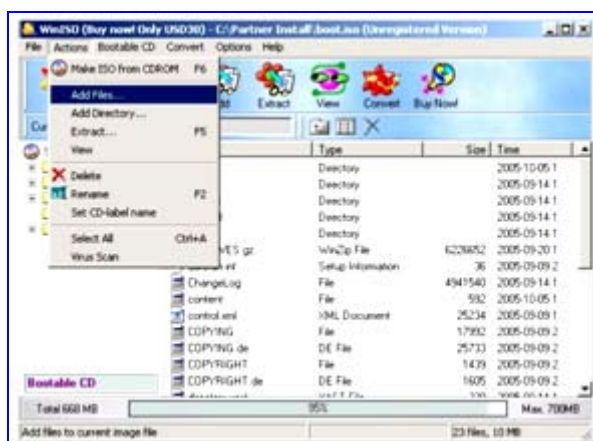
11. Save the changes to the *isolinux.cfg* file, and then close the text editor.
12. Open the 'Partner Install' folder and with the ISO edit utility, open the *boot.iso* file.
13. Navigate to the *isolinux.cfg* file, right-click it, and then from the shortcut menu, choose **Delete** to delete this file.

Figure 15-29: Deleting CFG File



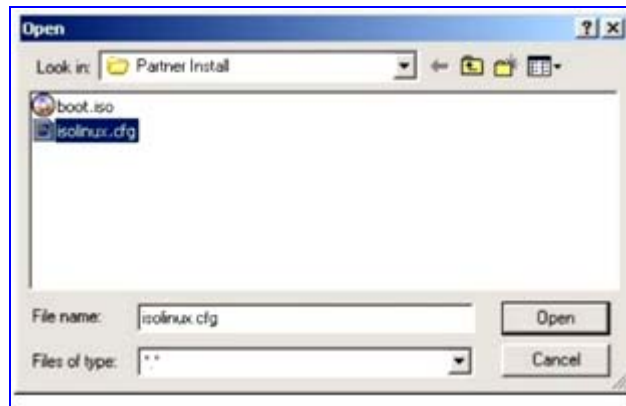
14. From the ISO edit **Actions** menu, select **Add Files**.

Figure 15-30: Add CFG File



15. Navigate to the 'Partner Install' folder, select the *isolinux.cfg* file, and then click **Open**.

Figure 15-31: Partner Install Folder



The updated *isolinux.cfg* file is added to the 'Partner Install' folder.

16. Save the *boot.iso* in the 'Partner Install' folder.

Figure 15-32: Save boot.iso



15.5.5 Stage 4: Burning the CD

- To burn the CD image, take these 3 steps:

1. Open a burning utility.
2. Use the **Burn Image** option to burn the *boot.iso* to an empty CD media.
3. Mark the media as the "Boot CD".



Note: Ensure that the *boot.iso* file should be burned as an image and not as a data file.

15.5.6 Stage 5: Installing the Boot Media

Now you have the boot media which enables SUSE installation of the Mediant 1000 using serial connection (terminal) with RS232 cable.

➤ **To complete the installation, take these 8 steps:**

1. Connect your Windows™ PC to the Mediant 1000 using a serial cable.
2. Open the Terminal application on your Windows™ PC. (Refer to the Additional Requirement in 'Additional Requirement for Linux & SUSE Installation' on page 516). Create a new connection with the following:
 - Connect Port = COM1
 - Baudrate = 115200 (or bits per second)
 - Data Bits = 8
 - Parity = None
 - Stop Bits = 1
 - Flow Control = None
 - Terminal settings = 132x47, ANSI Color (optional)



Note: If you are using Tera Term, navigate to the “Setup” option in the main menu and use the following configuration.

- Serial port:
>> Baud rate: 115200
- Terminal Setup:
>> Terminal size: 132x47
>> Term size = win size
>> Terminal ID: VT100
- Window:
>> Scroll buffer: 47
- Font:
>> Font: Terminal
>> Size: 8 (the default size is 10. If the window “slides” beyond your display then set the size to 8).

3. Connect the USB CD-ROM device via USB cable to the Mediant 1000.
4. Insert the “Boot CD” into the USB CD-ROM.
5. Power up the Mediant 1000.
6. On the Terminal screen, the BIOS phase starts and the Linux™ installation begins. The installation uncompresses the kernel, loads it and its drivers and starts the interactive installation.

**Notes:**

- After the BIOS phase, some badly formatted text may appear on the screen.
- From this point on, you should proceed with the screen instructions as instructed by your Linux distributor.

7. During the installation process, the system may reboot at some stage. In this case, remove the CD from the CD-ROM device.
8. During the installation of the fifth CD, the following items should be configured:
 - Username and password.
 - Firewall configuration: In the 'firewall selection/configuration' screen, select **Firewall: disabled**. In some distributions, you may have to select the **Change** option and set the configuration to 'manual'. This disables the firewall.
 - Network interfaces: The installation sets your network configuration to DHCP by default. If you plan to connect to the system immediately after the installation you'll either have to know the IP address assigned to you by the DHCP or set a **static IP address, subnet mask and default gateway**.

After the whole installation has been completed, you will be able login to the system from the serial console and/or to 'ssh' on your Mediant 1000 (to create an SSH remote connection to it) and to continue its post-installation configuring. You can use the boot media you have created to install multiple Mediant 1000 stations.

SIP**Mediant 1000**

User's Manual Version 5.2

